Dean A. Gratton

dp

Developing Practical Wireless Applications

COMMUNICATIONS

Developing Practical Wireless Applications

This page intentionally left blank

Developing Practical Wireless Applications

Dean A. Gratton

ELSEVIER
DIGITAL
PRESS
Amsterdam • Boston • Heidelberg • London • New York • Oxford
Paris • San Diego • San Francisco • Singapore • Sydney • Tokyo

Digital press is an imprint of Elsevier
30 Corporate Drive, Suite 400, Burlington, MA 01803, USA
Linacre House, Jordan Hill, Oxford OX2 8DP, UK

All illustrations created by Dean A. Gratton.

Library of Congress Cataloging-in-Publication Data
Gratton, Dean A.
Developing practical wireless applications / Dean A. Gratton. – 1st ed.
p. cm.
Includes bibliographical references and index.
ISBN-13: 978-1-55558-310-1 (pbk. : alk. paper)
ISBN-10: 1-55558-310-5 (pbk. : alk. paper)
1. Wireless communication systems. 2. Product management. I. Title.
TK5102.G75 2006
621.384–dc22
2006023176

British Library Cataloguing-in-Publication Data
A catalogue record for this book is available from the British Library.

ISBN 13: 978-1-55558-310-1
ISBN 10: 1-55558-310-5

For information on all Digital Press publications
visit our Web site at www.books.elsevier.com

Printed in the United States of America
06 07 08 09 10 9 8 7 6 5 4 3 2 1

It takes just one person to believe in you to make a difference; for me that's Sarah, my wife. With her continued belief in me I can truly fly.

To Henry John Camden:
the ideas we could have shared!

“The future success of wireless technology rests upon it becoming as overlooked as electricity.”

Gratton, D. A., 2006

Contents

About the Author

Dean Anthony Gratton is an independent technology consultant and author. He has worked within the communications industry for over ten years and has undertaken consultancy for a number of high profile companies to include Philips Consumer Electronics, TDK Systems Europe, Alcatel Microelectronics, Plantronics Inc., Sony and 3Com Europe. Dean has also been an active contributor to a number of technology committees. Furthermore, his work on defining new aspects of wireless technology has been patented and he is recognized as one of the leading authorities on wireless application development and visionary engineering. Dean is the author of a number of articles and papers as well as several bestselling books on wireless technology: *Marketing Wireless Products*, Butterworth-Heinemann (an imprint of Elsevier), 2004 and *Bluetooth Profiles: The Definitive Guide*, Prentice Hall PTR, 2002.

what is **wireless**?

You can contact Dean at *www.whatiswireless.co.uk*.

Preface

I wanted this book to challenge the fundamental foundation upon which the notion of wireless technology development rests. It seems that all too often manufacturers base their technology development on an inevitably faded blueprint of their peers' success: "Look, they're doing it, why aren't we?" Used, as a mission statement, it undoubtedly paves the way towards a future uncertainty where its adopters will fall into the cracks. All too keen on finding that elusive killer application, manufacturers are forgetting that wireless is still new; still finding its way. I have to confess that I am still unsure of its application base – it is, after all, easy to forget that a cable at best is a simple technology: you plug one end into Device A and the other into Device B. In an attempt to replace the infringement of cables with the true freedom of wireless, it escapes many manufacturers that, in making a product *wireless*, we often introduce an unmeasured level of complexity and, dare I say, cost to the consumer which we are still struggling to overcome.

I have come across some senior company individuals whose sheer ignorance has distorted the bigger picture of what needs to be realized. A singular vision driven by an underlying passion is an attribute lacking in a great deal of companies within the wireless industry. Many seem to adopt a knee-jerk reaction to product development: "The man who follows the crowd will usually get no further than the crowd" (Alan Ashley Pitt). This lack of innovation and child-like mimicry affords some companies a short-term lifeline of support, but inevitably sustaining a life support system of a lifeless and brain dead company is futile. I'll touch upon that elusive killer application again; it needs to be a clear winner for most companies. They are often reluctant to invest in a product that they are unsure about, nevertheless there is a nagging market trend indicating that there is (or is going to be) a strong demand – so who'll be the first? "Look, *they're* doing it, why aren't we?" and then they miss out on a commanding share of the market because they hesitated. I'll pause for a moment and ask you to consider what particular wireless product on the market strikes you as the most popular choice with consumers? Don't spend too much time thinking about it – it should just come to you. Once you have it there in your mind, ask yourself why that particular company has succeeded in their task of bringing something new and exciting to the marketplace? The answer, when explored more deeply, will almost certainly I assure you lie in one word: *confidence*. That is, confidence in the market and confidence in themselves as a group of innovators and educated risk takers. It may sound very contrived, but in an industry shrouded in hesitation and uncertainty it undoubtedly comes down to "who dares wins" in terms of product exposure and ultimate revenue success. The days have passed where consumers are avid loyal customers of branding – consumers want good value for money.

It is clear there are numerous wireless technologies each overlapping in application areas, but equally there is an accompanying list of reasons as to why you should choose one over another. *Developing Practical Wireless Applications* describes the most popular standardized technologies along with a set of proprietary technologies. The latter set is provided to challenge our belief in standardized technologies. I have often suggested that a proprietary technology will do the job – now! If you are selecting a technology that is unique to particular application and/or context do you really need it to interoperate with a huge device base across manufacturers? If not, a proprietary technology is most often available.

In comparison, a standardized technology assures us of interoperating across a large consumer base, enabling one manufacturer to confidently interoperate with another. The processes associated with such a technology can at times be perceived to be protracted and ambassadorial, but sustaining persistence will reward you with a well-balanced and distinguished product labeled with alluring accreditation.

I have been faced many times with such a dichotomy, but equally I have made choices that have been associated with a tried and trusted notion of belief and passion. There is never a magic answer but the very best that I can provide to you is that born of confidence.

Acknowledgements

I find myself writing my third book, completely aware of the responsibility, effort and time that it consumes out of my everyday social playtime. Some friends and family say that I'm committed and, alas, I confess I should be. But, without their support and guidance I would not be able to see yet another project like this through. I have to thank first and foremost Theron Shreve for his incredible saint-like patience and support.

I would like to thank all my family and friends for their unquestionable and unquantifiable support in guiding me and supporting me during this project – I need this, as I'm sure, inevitably, there will be another! It is evident that you are proud of me and I thank you so much for all your unconditional love.

On a more formal note, I would like to thank Dan Cui et al. of Aura Communications (www.auracomm.com), Ricco Borring of ZenSys (www.zen-sys.com) and Ed Rebello and Don Parkman of Cypress Semiconductors (www.cypress.com): thank you for your support and your patience.

Finally, I would like to thank the following for their support and technical guidance: Antonio García Gómez and Erwin de Witte of Philips Consumer Electronics (Leuven, Belgium). My ex-colleagues (and life-long friends) have afforded me a unique sanity check mechanism. And, I should mention Philip Loubele, also from Philips CE, for the Hong Kong experience: measure life in accordance with the parameters of the programme and when applicable, the Winnie specials! Sarah still doesn't remember falling off that stool!

Introduction

It seems somewhat paradoxical that we feel obligated to create a new wireless product that will simplify our experience in some part of our business or private life. With a new wireless technology in mind we dutifully begin brainstorming to determine what we will ultimately create. On occasions the direction we take seems to be mired as we quandary over the value added proposition for the consumer. What benefit will it really bring? And, why ultimately should the consumer pick it up from the shelf and place it onto the counter ready for purchase? A sense of practicality needs to be injected into the whole 'making wireless products' process as we choose to drive the future of wireless development forward. In that respect, *Developing Practical Wireless Applications* will guide the most eager of developer, the most fervent of business analyst, the most enthusiastic product planner and the most politically focused manager through choices in respect of which wireless technology to use. Ultimately, this book will guide you through each technology with an aim to enable you to make an educated choice regarding your would-be wireless product. Furthermore, you will glean from the subsequent chapters a detailed breakdown of each technology. In some places you will find exposure, right down to the deepest of layers, enabling engineers to understand the inner workings of each technology, whilst intermediate readers will enjoy an understanding of the peripheral discussion surrounding a technology.

Our understanding begins with Part One, *Understanding a Wireless World*, where we attempt to question our basic premise in Chapter 1, *Making Sense of Wireless Technology*. It seems that most consumers are unable to escape from the marketing onslaught, but with such wealth of information and choices how do we make sense of it all? In Chapter 2, *Understanding the Wireless Audience*, we generalize the consumer audience into demographics in an attempt to understand their purchasing motivation and behavior. Conversely, Chapter 3, *Comparing Wide-area and Personal-area Communications*, illustrates two important concepts in the arena of wireless technology, namely, personal-area and wide-area. Here we compare such epics as Bluetooth, ZigBee and WiFi alongside the more traditional 2G, 2.5G and 3G technologies. In Chapter 4, *Can we Confidently Rely on Wireless Communication?* we begin to address issues surrounding security, interference, coexistence and interoperation which continue to plague our ethos of working and social life. In Chapter 5, *Realizing a True*

Wireless Life-style Vision, we explore the future of consumer interaction and how we might achieve true transparency and complacency with wireless products – in essence we touch upon how a wireless life-style should manifest itself to the consumer.

With our foundation set and our expectations defined we can now continue our understanding with a series of chapters that aim to help us appreciate that a wireless technology doesn't have to be governed in a rigorous manner with copious quantities of red tape. Part Two, *A Proprietary Approach to Developing Wireless Applications*, presents three technologies that deliver wireless communications in an unpretentious fashion. Firstly, in Chapter 6, *An Introduction to the Notion of Proprietary-based Wireless Application Development*, we make light of the standardization process and present our three case studies. In our first look at a proprietary technology, Chapter 7, *ZenSys: An Open Standard for Wireless Home Control,* discusses a new wireless home control technology enabling all types of homes with automation, control and security. Secondly, in Chapter 8, *Cypress Semiconductor: Introducing WirelessUSB*, we illustrate the advantage of utilizing a technology that enables wireless functionality through a standard USB port. Cypress Semiconductors took advantage of the 2.4GHz ISM band to deliver a cable replacement technology that confidently competes with Bluetooth. In the last chapter of this section, Chapter 9, *Aura Communications Technology: Creating the Personal Bubble*, we witness a unique technology that is capable of delivering wireless stereo audio for personal audio players.

In the final section, Part Three, *A Standards Approach to Developing Wireless Applications,* we draw upon the numerous technologies that we have undoubtedly come into contact with. In Chapter 10, *An Introduction to the Notion of Standards-based Wireless Application Development*, we refocus our discussion in light of the benefits received from adopting a standardized approach to wireless product development. In Chapter 11, *Bluetooth: A Cable Replacement Technology,* we discuss and illustrate a technology that has been around for a few years but still is very much in its infancy in terms of market penetration. Equally, in Chapter 12, *ZigBee: Untethered and Unlicensed*, we introduce a relatively new technology that hopes to become a de facto home wireless control solution for all types of home. In Chapter 13, *WiFi: Enabling True Ubiquitous Connectivity*, we discuss a technology that has been swept away with insurmountable success and draw witness to one that has penetrated a large consumer base of electronic products. In Chapter 14, *Near Field Communications: The Smart Choice for Enabling Connectivity*, we illustrate a unique and ingenious wireless medium that could revolutionize the way in which consumers interact and enable wireless products. In our final chapter, Chapter 15, *Ultra-Wideband: Introducing a New Short-Range Wireless Medium*, we introduce a technology that could either witness the demise of Bluetooth, or through a unique alliance may pave the way to Bluetooth dominance.

This page intentionally left blank

Part One

Understanding a Wireless World

This page intentionally left blank

1

Making Sense of Wireless Technology

Wireless communications have been in existence for over one hundred years and have had an innocuous impact upon our everyday or working lives in one form or another. From the earliest radio sets to infrared remote controls and cordless telephones, evolving into the digital mobile era, wireless products have radically influenced the way we now choose to live and work. Yet, until *new* wireless emerged, the concept of *wireless* itself remained firmly associated with images of old-fashioned radio boxes playing popular music or broadcasting the news. The introduction of a new generation of wireless technologies has well and truly challenged our founding belief. Mention wireless today and people are more inclined to think of cellular, infrared-, Bluetooth- and WiFi-enabled devices than that old wireless box in the corner of their grandmother's kitchen.

In this chapter we will examine the current status of wireless technology and question the originality of new (or personal-area) wireless products. We find ourselves surrounded by a technology that has come to affect the way we live and work, although still remains an experience that varies from individual to individual. Primarily, the influence of wireless depends upon numerous scenarios, coupled with varying types of exposure and environmental facets. When analyzing this context, end-users and companies alike lean towards certain (business) models which, in turn, justify their purchase or non-purchase of wireless-enabled products. Ultimately, these models may have an attached financial, practical, usability or security factor, which is channeled into a decision-making process – and this is something we will discuss later on in the chapter. In the immediate sections that follow, we ask pertinent questions about wireless technology, some of which may begin to lift what may become the lid of Pandora's box. But to make real sense of it all we need to be clear in our own minds about why we have and are using wireless technology, and this chapter entertains ambivalent thoughts we might secretly share, but not necessarily disclose to our peers and superiors.

Those among us who have endured the constant stream of emails and flyers through the post box inviting us to attend an exhibition or conference may have experienced instances of déjà vu. Perhaps with these personal experiences we may wrangle with the notion of understanding a purpose of wireless being. More specifically, the excitement of attending a new wireless exhibition and conference can often be likened to an evening at home in front of the television. You look forward with eager anticipation to a new episode of your favorite programme, only to discover that you are watching a re-run. With a homage akin to a frequent ritual and sacrifice, you religiously tune in every week, say your prayers, and ask God to bless John Logie Baird for his foresight and ingenuity. Unfortunately, with a repeat of the previous episode and coupled with your unduly sacrifice, you still sit down and watch the ever-so familiar programme; although this time you're able to watch it more critically realizing to your dismay that the plot is thin and tiring. Naturally, you begin seeking recompense.

In each episode there are new faces, naturally with a new story to tell. But, the over complicated interwoven tapestry of a plot only reminds you of the eighth episode in series one where Carrie found her teenage love sweetheart, Ben in bed with her best friend Michael – someone save us please!

There is such an unnerving crossover and painful familiarity with our frequent exhibitions and conferences. In essence, the annual, bi-annual and quarterly gatherings are a complete rehash of what we've already seen. Inextricably, we often pay inflated delegate prices to watch a re-run of "How to Develop Wireless Applications with Java API set v26.42;" after all, last quarter you witnessed how to develop the same applications with v22.14. Similarly, like a religious congregation, its followers attend technology exhibitions in an attempt to discover a wealth of new wireless products. However, these dedicated worshipers are reminded of products that seem to be a re-hash, or perhaps the box has seen a subtly amended product feature list. This may be an unfair or harsh critique, but here we are trying to emphasize the need for original new product ideas.

Nevertheless, next time your boss agrees to pay for a delegate's pass to a conference or exhibition remember to be as critical with the range and diverse collection of conferences as you were with the haunting eighth episode. You now unavoidably recall the image of Carrie's face of horror followed by disappointment where her final thought rested with a shocking notion of curiosity – let's not go there. Moreover, the relevance of this well-drawn-out and exhausted analogy is to remain objective about your needs as well as your consumers. Let's provide effective added value to our products whilst generating new technology because there is an obvious need. Ultimately, we need to apply a sense of proportion and reality.

Where are We Today with New Wireless Technology?

Suitably equipped with some sense of proportion and reality, this is what we are led to believe about personal-area wireless technology: a wireless-enabled office or home, or indeed a portable wireless-enabled product, such as a cellular phone or *Personal Digital Assistant* (PDA) bestowing ease-of-use, seamless operation and transparency and an unmeasured sense of freedom. Does this exist today?

Companies advocating wireless technology insist that the technology itself is safe and reliable, and should be deployed in most cases, as opposed to a fixed infrastructure. Remember, wireless technology should be typically utilized in an area where a fixed infrastructure would normally be difficult to implement. Moreover, there is a striking cost–benefit in implementing wireless, as the availability of wireless products is now very prevalent. Does your company have a wireless infrastructure or at least a combination of fixed and wireless? If you can answer yes to this, then ask yourself this final question: is it connected to the wider company network where potentially it has access to company confidential information? Your thoughts are coming through loud and clear!

Ironically, let's draw our attention to the sensationalized security scares: *WarChalking* and *BlueJacking* are two current examples. A breach of security means that hackers and the like can gain access to confidential information (we will discuss the issue of security in more detail in Chapter 4, *Can we Confidently Rely on Wireless Communication?*). These sensationalized stories portray the poor security and unreliability aspects of the technology; is this the fault of the manufacturer or perhaps a result of the ill-educated user/administrator not configuring the products appropriately?

Standards bodies actively assure us that security concerns are a thing of the past and, of course, setting them up is a matter of simple configuration – anyone can do it! You may already be aware that a standards body is an organization that undertakes the responsibility (that is, general maintenance, future growth and so on) of a specification for a particular wireless technology. In fact, there are as many standards bodies and groups as there are wireless technologies.

On occasions we may have witnessed several wrestling matches engaged by manufacturers and standards organizations. In a paradoxical context, a large majority of the standards organizations are made up of many manufacturers, all striving for the same goal, but with a series of political agendas. One common and, often, harmonious driving issue that many manufacturers discuss is that of interoperability, that is, where one manufacturers product successfully works with another manufacturers. For example, one manufacturer may provide an *Access Point* (AP) and another the client device enabling a notebook to connect to a *Local Area Network* (LAN).

Reasons for Choosing Wireless

Let's take this opportunity to combine our positive and negative thoughts regarding new wireless technology and attempt to rationalize its potential deployment, alongside the plethora of other gadgets that most of us already use. Does a company really need to implement a wireless infrastructure? In answering this particular question let's refer back to our earlier identified key factors, such as financial, practicality, security and so on. Undeniably, these fundamental factors form part of the decision-making process. We have already acknowledged that the financial aspect of implementing such an infrastructure is nowadays significantly cost effective, as the availability of wireless-enabled products is widespread and, naturally, the cost is proportional to the size of a company. We have witnessed many notebook and desktop manufacturers offering integral wireless solutions that are ready to go and require minimal configuration. Some companies may choose to purchase a PCCard- or USB-based product to metamorphosize their standalone computers into the new wireless generation. Again, these products are commonplace, but who will support this new infrastructure? Many companies specialize in the implementation and deployment of such infrastructures and are readily available to assist. However, consideration of this kind of outsourcing needs to be added to the overall projected cost of deploying and implementing such an infrastructure. Nowadays, a significant number of companies have their own internal IT departments where several administrators may manage wireless deployment and subsequent maintenance. This approach is a practical solution and will help reduce the overall financial outlay within a company. However, consideration needs to be given to possible retraining within the related IT department.

We've already considered a company's predicament regarding the transition to wireless, but what about ordinary users? Moreover, what about the practical usability and user friendliness of the many wireless products on offer: how will users react to this new technology? Will they find the educational aspect of adopting a new wireless product a chore? To many of us, there is a sense of initial eagerness, coupled with frivolity as we unwrap the product, put aside the packaging; scan the accompanying software CD and observe the product in 3D in our hand. Most of us may decline our initial thought of "let's put it in and see what happens," and succumb to picking up the manual and coming to terms with the *three letter acronyms* (or TLAs – how tedious!). With this in mind, we need to ask ourselves: are any learning curves easily justified through the introduction of a new wireless product that claims to simplify one aspect of our life? Were we already comfortable with using the snake-like cables which, initially, seemed like a black art to master; or do we find that the introduction of a technology such as Bluetooth, with its abracadabra-like magic wand, has wirelessly tapped the top of our notebook three times wishing the cables away?

Where is the Original Thought?

It is clearly evident that most of us (companies and individuals alike) have formulated our own conclusions regarding the positive and negative aspects of new wireless technology.

We talk of configuration issues and how difficult it is moving from one network to another. But, whether we choose to accept it or not, manufacturers (and their marketers) are committed to seducing us all into adopting and embracing its alleged benefits. This leads to another important question: are manufacturers creating wireless products unnecessarily, is their marketing tainted with hyperbole and – let's be honest – do we really need them?

With manufacturers' new spin: "look, it's wireless," can they sometimes be guilty of reinventing the wheel? We often witness an increasing number of pop bands covering old classics and reinventing them as their own. Are manufacturers similarly guilty of a lack of originality with their wireless products? Where is the original thought? We find ourselves replacing infrared in a remote control with Bluetooth or ZigBee as another new technology, accompanied with yet another marketing spin: "Look, you can now change the channel on your TV from the kitchen." Is this a cynical perspective? Perhaps. But we shouldn't be afraid to ask questions. What's wrong with playing devil's advocate? Let' s choose to be practical about our approach to new wireless technology. After all, developing the right product for the right kind of market will undoubtedly create a new way of thinking for consumers and, in turn, they will become our judge and executioner regarding its success or failure. But oddly enough, most manufacturers choose to ensure that a product released on the market has satisfied the demographic; they are no longer taking risks – they need a sure thing. With a degree of educated certainty and no matter how much money you invest into a new product, ultimately the consumer *will* decide. Should we therefore rely on consumerism and its behavior to bias our sense of proportion and reality?

A New Way of Thinking

Perhaps the marketers that exploited the intricacies of the technologies by associating the *without wires* factor with the innate capabilities of wireless have brought about this radical change in perception, or perhaps we, as consumers, have created the transition of association ourselves through a need to condense our growing fascination with mobility, freedom and time conservation into a single word. How awful, we've reached an era of manufactured needs: on the one hand we have the marketers telling us that we need this product to aid and abet in our lives, whilst on the other we were already managing perfectly well without it. Most likely the change was brought about through a combination of the two, but it marks a clear boundary between wide-area and personal-area generations of wireless technologies upon which (the latter) this book is primarily based. This change has inescapably brought about a new way of thinking.

In making sense of wireless technology, we have posed positive and negative questions to ourselves and internally wrangled with the financial, usability, security and practicality factors. “Just as these facets are unique to a company or user, it is predicted that, as we become more active in the future of wireless, along with its anticipated longevity in the marketplace, financial constraints will diminish; usability will surely become simpler and adoption will become wider. But let’s not allow this to become “complacency for complacency’s sake,” as we should always take the devil’s advocate stance. Wireless technology has become an effective communications tool. Communication is the heart and soul of every business and while we remain connected we continue doing business. It has also enabled us to communicate over great distances. For instance, families separated by continents remain in contact through wireless technology, whether it’s wide- or personal-area, or indeed a combination.

Primarily wireless technology is marketed as a tool that promotes mobility, transparency and freedom, enabling users to roam from office, to café or restaurant and even to the beach. But just a moment! Surely we escape to a restaurant or to the beach with an aim to banish the constraints of the working day? Although, if you are able to visit a beach or enjoy a meal with fellow colleagues in a restaurant whilst perusing some forecasts, then it doesn’t seem that bad an idea. Does it?

Summary

- Wireless technology has surrounded us for over one hundred years.
- Personal-area wireless technologies have entered into certain aspects of our living and working lives.
- The founding concept of wireless conjured up images of a radio set in the corner of your grandmother’s kitchen.
- Nowadays, consumers are more aware of new wireless technology and, as such, have moved away from the traditional notion of wireless.
- The influence of wireless depends upon numerous scenarios, coupled with varying types of exposure and environmental facets.
- End-users and companies lean towards certain business models which, in turn, justify their purchase or non-purchase of wireless-enabled products.
- These business models may have an attached financial, practical, usability or security factor, which is channeled into a decision-making process.
- We need to be clear in our own minds why we have and are using wireless technology.
- What we are led to believe about wireless technology is based on the concept of an environment that bestows ease-of-use, seamless operation and transparency.

- Companies advocating wireless technology insist that the technology itself is safe and reliable, and should be deployed in most cases.
- There is a striking cost–benefit in implementing wireless, as the availability of wireless products is now very widespread.
- Standards bodies actively assure us that security concerns are a thing of the past.
- A driving issue that many manufacturers discuss is that of interoperability. Configuring some wireless networks can be cumbersome to set-up.
- Fundamental factors such as cost form part of the decision-making process.
- The cost of setting up a wireless infrastructure is proportional to the size of your company.
- Many manufacturers integrate wireless within their notebooks and desktops.
- Companies may choose to purchase a PCCard- or USB-based product to expand their wireless infrastructure.
- Some companies may outsource their implementation and deployment of a wireless infrastructure.
- Outsourcing of this nature should be added to the overall cost.
- A significant number of companies have their own internal IT departments where several administrators may manage the wireless infrastructure.
- Ordinary users are also faced with practical usability and user friendliness factors when deciding to purchase a new product.
- As individuals we will have already formulated our own conclusions regarding the positive or negative aspects of new wireless technology.
- The adoption of new wireless technology has inescapably brought about a new way of thinking.
- Are manufacturers creating wireless products unnecessarily?
- Developing the right product for the right kind of market will undoubtedly create a new way of thinking for consumers.
- In turn, consumers will become our judge and executioner regarding a wireless product’s success or failure.
- Undoubtedly, financial constraints will diminish; usability will become simpler and adoption will become wider.
- Communication is the heart and soul of every business and while we remain connected we continue doing business.
- Primarily wireless technology is marketed as a tool that promotes mobility, transparency and freedom, enabling users to roam from office, to café or restaurant and even to the beach.

2

Understanding the Wireless Audience

This chapter has its roots in consumer psychology for a very good reason. Successful product development begins first and foremost with building a comprehensive understanding of the market for which your products are intended or, put more simply, “give them what they want and they will come back for more.” You may recall from our first chapter (Chapter 1, *Making Sense of Wireless Technology*) that consumers are our judges and executioners regarding the success or failure of a product. Our primary objective in this chapter is to shine some light on the consumer psyche and, perhaps more importantly, to move this light around so as to illuminate and expose the deep crevasses within (see Figure 2.1); in turn, we will begin to build an appreciation of how, why and what key influences are used in the consumer decision-making process. We will then be more successful in attempting to categorize consumers by age, motivation, income and usage scenarios. From this foundation we can begin to truly understand today’s wireless audience.

We try to find purpose and direction for all areas of our lives. From setting up a home to running a business, we all internalize the procedures that govern our choices and behavior and place these into clearly defined mental boxes, formed through a combination of past experience and the practical opportunities that face us. The problem with these boxes is that they are, all too often, walls without doors. Confining us into a set of expectations and behavior patterns that stretch our limitations as partners, parents and employees and becoming more like prisons than the ordered sanctuaries we had formed them to be.

For today’s consumers, wireless technology offers us an extraordinary liberation. Utilizing wireless technology allows us to finally place doors into our walls and merge internalized boundaries into one another as we are introduced to new levels of portability and freedom, both at home and in the workplace. In our previous chapter we illustrated that many of us could now choose to work in a café or restaurant, whilst maintaining a disciplined ethos, alongside a flexible working environment.

Figure 2.1 *The human psyche: the collection of neurons with each synaptic exchange and the mass of energy released create an aurora of consciousness; in turn, our innate psyche.*

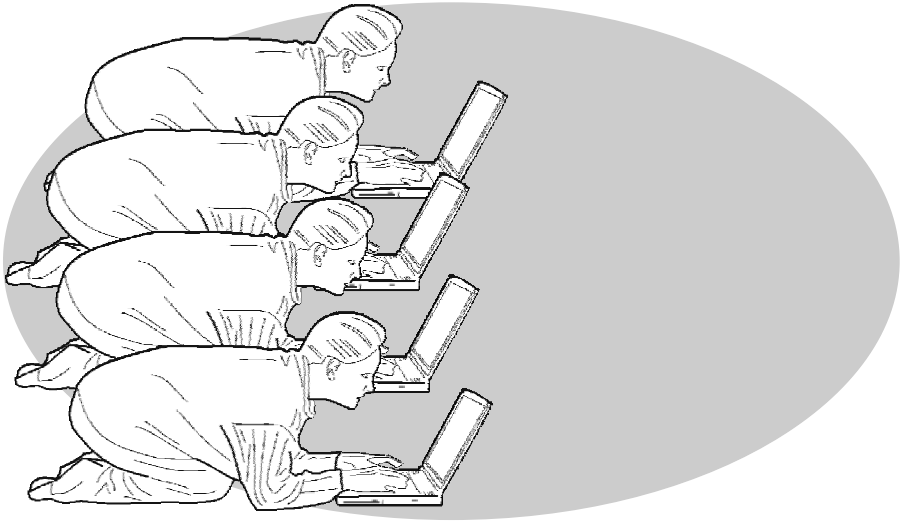
For many consumers, the concept of this kind of wireless liberty is a heady revelation, yet, amazingly, it is one that marketers have only recently begun to fully exploit. In the early days, the wireless manufacturers' marketing focus was very much on the technology itself and its physical attributes. We were blasted with numerous messages, telling us how new wireless technology worked and hyping its potential far beyond its initial capabilities, in a way that most consumers found intimidating and non-supportive of their life-style and expectations. One typical example is that of Bluetooth technology; Bluetooth was heavily marketed during 1999/2000 and promised to deliver extraordinary features, but at the time, the technology was nowhere near a satisfactory and stable completion.

Support is the key word here. To put a wireless product into a clear usage scenario for the consumer, it needs to be seen to provide a support structure for a particular aspect of their lives. A good example here would be the illustration of a mother sending and receiving emails from her *Personal Digital Assistant* (PDA) outside the school where she has just dropped off her children. This image combines the twin aspects of family and work responsibilities and allows the consumer to psychologically bridge the gap between the two through wireless functionality. With this in mind, when developing a new wireless application, we can see that defining its intended support attributes within clear usage scenarios is just as important as choosing the right wireless technology for the intended end product. In fact, one aspect will undoubtedly impact upon the success of the other.

Because of its innate attributes of mobility and freedom, the market for wireless products is extensive and spans from the rapidly evolving mobile youth market to the protection and security provided to the elderly through wireless home monitoring systems. Currently the biggest slice of the wireless spectrum is that of the mid-generation twenty-five to forty year olds, where work and home responsibilities make time a precious commodity. According to consumer watchers TrendWatch (TrendWatching.com), Internet access has become nothing less than *Online Oxygen*, with continual access being sought and considered a necessity by this particular segment of the wireless marketplace. Clever wireless manufacturers have responded to this need and are continually working to position a new religion of *hotspot* worship (see Figure 2.2) in every form of consumer outlet, from cafés to train stations; some 120,000 are predicted within the US alone by 2006. A hotspot provides the ability for users with a notebook computer or PDA to access the Internet or the office Intranet through a secure wireless connection. The WiFi Alliance (a non-profit international association formed in 1999) offers a comprehensive list of hotspot locations through their WiFi Zone program.

It isn't enough for us to be able to work from home anymore – today's most hearty wireless consumer craves the ability to work from anywhere and, perhaps more importantly, at anytime.

Figure 2.2
Hotspots are becoming the temples for new wireless worshipers.



And, when looking beyond our virtual workspace to other dimensions of our lives, particularly those of entertainment and education, the same holds true. The freedom afforded to the wireless executive extends out from the workforce to other areas of life such as entertainment and education. Today, our kitchens can become classrooms and our laundry rooms libraries. Some worry that old-fashioned family values are being swept away by the wireless tidal radio wave, whilst others revel in the freedom afforded to their families and embrace the diversity of living and working without wires.

Categorizing the Wireless Audience

In order to assist in both the initial development planning procedures and long-term market positioning of new wireless products, we need to clearly segment the market into distinct consumer groups, each assessed by motivation to purchase and typical usage patterns. As such, Table 2.1 to Table 2.4 detail the group market alongside their motivation to purchase an identifiable wireless product; their predominant usage scenario and their assumed level of income.

The Diffusion of Wireless Innovation

This term, *diffusion of innovation*, is particularly relevant when building an understanding of the new wireless audience, as it refers to the tendency for new types of products, practices or ideas to increase among people. Early adopters are crucial to a

Table 2.1 *Group One: Youth Market between 12 and 24 Years*

	Description
Motivation	Peer cohesion and a sense of belonging, individuality from other groups in terms of style and usage models with an emphasis on entertainment and peer-to-peer communication.
Identifiable Product	Cell phones with interchangeable covers to allow for personalization between user groups, *Short Message Services* (SMSs) and *Multimedia Messaging Services* (MMSs) applications, integrated digital cameras, *third generation* (3G) video and gaming capability, ring tone bolt-ons.
Typical Usage	Pay as you go cellular phone accounts (low budgets with younger Group Ones). High levels of SMSing (or texting) and inbuilt gaming facilities.
Income Factors	High levels of expendable income Low levels of income

Table 2.2 *Group Two: Mid Generation Executives 24 to 55 Years*

	Description
Motivation	Career tracking, time control, the integration of work and pleasure, support systems (career and home), keeping up with technological advances, prestigious individuality.
Identifiable Product	WiFi integrated laptop or PDA, enabling hotspot access to the Internet and easy synchronization of data between home and office. Bluetooth-enabled cell phone to access the Internet or office when no hotspot is available.
Typical Usage	Portability means working "on the fly" with the anytime, anywhere access principles.
Income Factors	Mid to high levels of expendable income Mid to high levels of income

Table 2.3 *Group Three: Mid Generation Non-Executives 24 to 55 Years*

	Description
Motivation	Time control, financial constraints, long-term security.
Identifiable Product	Bluetooth-enabled cell phone and headset.
Typical Usage	Communicating with work, home and family – usually on a pay as you go or economy fixed monthly package.
Income Factors	Low levels of expendable income Low to mid levels of income

Table 2.4 *Group Four: Older Generation 55 Years plus*

	Description
Motivation	Safety and security.
Identifiable Product	Wireless health monitor necklace and wall-mounted transceiver.
Typical Usage	Inbuilt alert system – touch activated on necklace, allows for rapid response from warden/care authorities to which the system is linked. Contact will be made via the transceiver to check on the status of the wearer whilst help is sent.
Income Factors	Dependent upon previous income levels/savings/pensions and so on.

product's market success as they will generate group interest among other social and peer groups, resulting in a well received wireless product being embraced and accepted by a wider range of users.

Wireless technology is a *dynamically continuous* innovation due to the fact that it is constantly evolving and adapting to new types of application and usage models. Visionaries, engineers, managers and investors need to ensure that the evolution of their wireless applications is possible in a way that requires little or no re-education on the part of the user. Cost implications can play a part here and manufacturers inevitably benefit by understanding the impact these might have on the consumers' willingness to upgrade, by looking at wireless market adoption trends alongside demographic indicators.

Alongside the evolved practicalities of new wireless applications, many successful wireless devices have been developed and initially marketed through the creation of consumer needs. Factors such as *life-style* models, as depicted in our previous categorizations (see Table 2.1 to Table 2.4) in combination with a nurturing process by wireless product marketers, may result in aspirational needs being created in the minds of consumers. Early adopters then ensure that these life-style model needs are further reinforced within the target market, resulting in an increased diffusion of innovation.

Cultural Economic Effects on Product Pricing

The majority of wireless pricing research has been carried out on US consumers, which raises the potential issue of oversimplification in certain global-economic areas of theory. Evidence, however, exists of a strong correlation between quality and price in the mind of the UK and Japanese consumers whilst, in less developed countries, price does not necessarily have a strong relationship with perceived product longevity or quality of build and, accordingly, far less consumer brand loyalty exists. Differences in economic culture may therefore have a dramatic impact upon pricing and promotion strategies; for example, differences in income payment receipt can powerfully influence the effectiveness of a product's promotion when put into a set financial framing concept such as: "You can enjoy our latest 3G package for less than a dollar a day!" To a weekly paid employee, a dollar is seen as a larger slice of their paycheck than consumers who are paid on a monthly basis.

In the case of mobile application developers, building good relationships with carriers is key to ensuring that cultural needs and variances are built into new wireless applications. For example, gaming applications based upon the latest movie themes can be more easily managed when carriers are able to play a part in accurately promoting launch dates in accordance with appropriate media tie-ins and cinema release dates.

This process is of particular value to new developers, whose application adoption may be assisted by carrier association. In the US the carrier relationship is considered to be particularly valuable and this holds true in other countries as well. In the UK and the rest of Europe, however, distribution has a slightly different emphasis and much occurs through aggregators or portal sites.

A Long-term Perspective

To fully understand the wireless audience and be able to effectively develop the kind of new wireless applications that will achieve consumer success, we must be able to look, not only at the aspirations and needs of life today, but also to see beyond the "here and now" towards what might lie ahead. To do this we don't need a crystal ball or any kind of psychic abilities, but what we do need to be able to do is to take what we already know about the evolution of wireless technology and to combine this knowledge with educated intuition about the future. Trends are already beginning to show themselves in terms of wireless application take-up and we can further build upon these demographics to make intelligent predictions about where future development paths might lead us.

Summary

- Effective product development begins first and foremost with building a comprehensive understanding of the market for which your products are intended.
- Consumers can be categorized into distinguished groups with attributes such as motivation, age, income and usage scenarios.
- As consumers, we try to find purpose and direction for all areas of our lives; from setting up our home to running a business.
- We all internalize the procedures that govern our choices and behavior into clearly defined boxes, formed through a combination of past experience and the practical opportunities that face us.
- The problem with these boxes is that they are, all too often, walls without doors. This confinement turns our boxes into prisons rather than the ordered sanctuaries we had formed them to be.
- Wireless technology offers us an extraordinary liberty.
- Utilizing wireless technology initially activates the process of placing doors into our walls, where over time these walls begin to diminish.

- To many consumers, the concept of this kind of wireless liberty is a heady revelation.
- Marketers have only recently begun to fully exploit the real benefit of this wireless liberty.
- More and more wireless products are becoming supportive of our everyday needs.
- Nowadays, marketers are using clearer messages in their marketing.
- When developing a new wireless application, we can see that defining its intended support attributes within clear usage scenarios is just as important as choosing the right wireless technology for the intended end product.
- The market for wireless products is extensive and spans from the rapidly evolving mobile youth market to the protection and security provided to the elderly through wireless home monitoring systems.
- Wireless manufacturers are continually responding to the need of the consumer.
- It isn't enough for us to be able to work from home anymore – today's most hearty wireless consumer craves the ability to work from anywhere.
- And, when looking beyond our virtual workspace to other dimensions of our lives, particularly those of entertainment and education, the same holds true.
- The freedom afforded to the wireless executive extends out from the workforce to other areas of life such as entertainment and education.
- Today, our kitchens can become classrooms and our laundry room libraries.
- Some worry that old-fashioned family values are being swept away by the wireless tidal radio wave, whilst others revel in the freedom afforded to their families and embrace the new diversity of living and working without wires.
- We need to clearly segment the market into distinct consumer groups, each assessed by motivation to purchase and typical usage patterns.
- Diffusion of innovation is particularly relevant to understanding the new wireless audience, as it refers to the tendency for new types of products, practices or ideas.
- Early adopters of wireless technology are crucial to a product's market success.
- These early adopters will generate group interest among other social and peer groups, resulting in a well-received product that is embraced and accepted by a wider range of users.
- Early adopters also ensure that life-style model needs are further reinforced within the target market.
- Wireless technology is a dynamically continuous innovation due to the fact that it is constantly evolving and adapting.
- Manufacturers should keep re-education to a minimum.

- Cost is a significant factor for users wishing to adopt or upgrade.
- Differences in economic culture have a dramatic impact upon pricing and promotion.
- To understand the wireless audience we must be able to look, not only at the aspirations and needs of life today, but also to see beyond the "here and now."
- We don't need a crystal ball or any kind of psychic abilities.
- We do need to be able to take what we already know about the evolution of wireless and to combine this knowledge with educated intuition about the future.

3

Comparing Wide-area and Personal-area Communications

The era of wireless communications technology utilizing radio waves as a transport medium has enabled electronic devices to exchange a variety of data wirelessly, transparently and effortlessly. In establishing a new era of wireless technology enabling personal freedom and mobility has both distinctive parallels and contradictions to the older, more established wireless technologies. We should not forget that wireless technology emerged in the late 19th century. It was with Guglielmo Marconi's determination that saw the first broadcast of the human voice in around 1896. It wasn't until the 1940s that we saw the emergence of commercial digital wireless and cellular technology, but then it was still very much in its infancy.

Both *wide-area networks* (WANs) and *personal-area networks* (PANs) share a common radio medium in which data is transferred between electronic devices, but it is a combination of consumer perception and usage scenarios that distinguishes them. As we move forward in this chapter, we will clarify the distinction that can be made between wide- and personal-area wireless, alongside an in-depth discussion of the technologies that underlie most cellular-centric products. Additionally, we will consider the perception that most of us enjoy when we come into contact with wide- or personal-area technologies. We will discover that these technologies are, indeed, complementary and together provide some powerful applications. It is covered in the chapter as a means of providing a holistic perspective of the available technologies, whilst not detracting from our primary focus.

Wide-area vs. Personal-area

The more established or wide-area technologies, such as cellular and satellite, are tried and trusted communication technologies that have been around for many years.

We've come to know wide-area communications as *telecommunications*, since wide-area is synonymous with connectivity over greater distances. Typically, in this context the user has been able to establish a level of familiarity where the wireless capability is no longer the perceived application. Distance is no longer an issue and no longer is wireless technology concerned purely with wide-area communications, as in the case witnessed by Marconi's eagerness to transmit radio waves over the Atlantic Ocean. Nevertheless, with Marconi's perseverance he achieved societal cohesion by bringing communities together over great distances. Incidentally, he also brought about a standardization that enabled the international maritime services to adopt his technology, as an effective communications method for naval vessels at sea. Similarly, telecommunications are prevalent in all sorts of infrastructures and in Figure 3.1 and Figure 3.2, we illustrate some of the technologies that characterize wide-area communication.

Nowadays, *new* wireless technology focuses primarily on personal-area communications, with the introduction of a new range of wireless-enabled applications that, in turn, define a greater sense of personal mobility and freedom that uniquely captures the personal-area technology era. Technologies such as Bluetooth, WiFi, ZigBee and so on, afford the user greater flexibility in their personal and/or working environment. Personal-area technology enables users to create their own personal communications environment, which may comprise a notebook wirelessly connected to a network and a cell phone that utilizes a Bluetooth-enabled headset. In Figure 3.3 and Figure 3.4 we demonstrate some of the technologies that may comprise personal-area communications. In the latter example we can see how wide- and personal-area communications

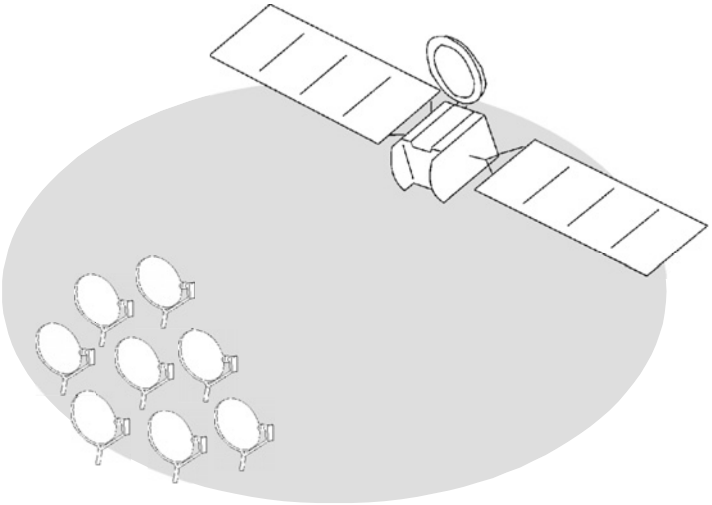


Figure 3.1
The depiction of wide-area wireless communications comprises the ability to exchange data over distance. In this example we can see that a satellite in earth's orbit can reach many receivers.

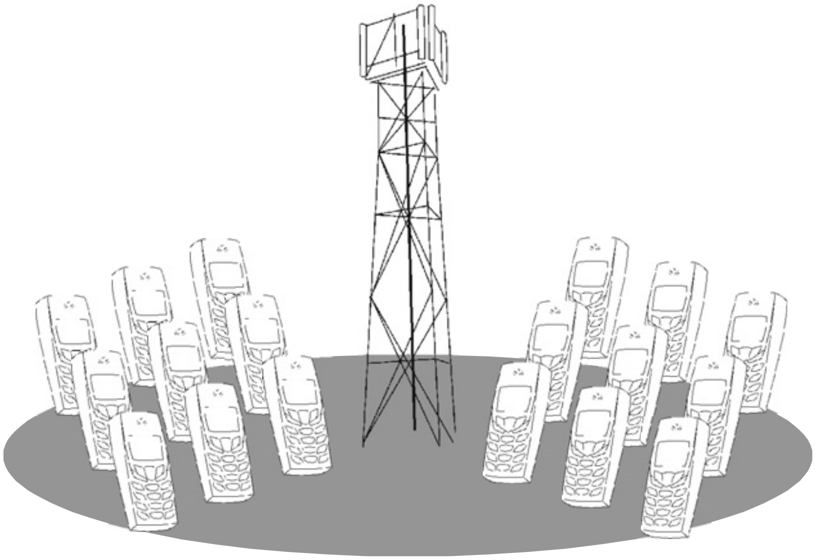


Figure 3.2
In this depiction of wide-area wireless communications we can see that a cellular base station is capable of servicing many cellular phones.

overlap, where the combination of a personal-area environment utilizes the wide-area (or telecommunications) infrastructure enabling a user to exchange data over distance.

One clear distinction between these technology types is the complacency that a user establishes with a product over a period of time; we touched upon this earlier. This familiarity breeds complacency towards the intended wireless device. In other words, do we perceive a cell phone as a wireless-enabled product? Indeed, the cordless

Figure 3.3
A personal-area network comprises the collection of electronic devices that typically communicate over a relatively short distance. In this example, a user has a Bluetooth-enabled headset along with a cellular phone, notebook and PDA.

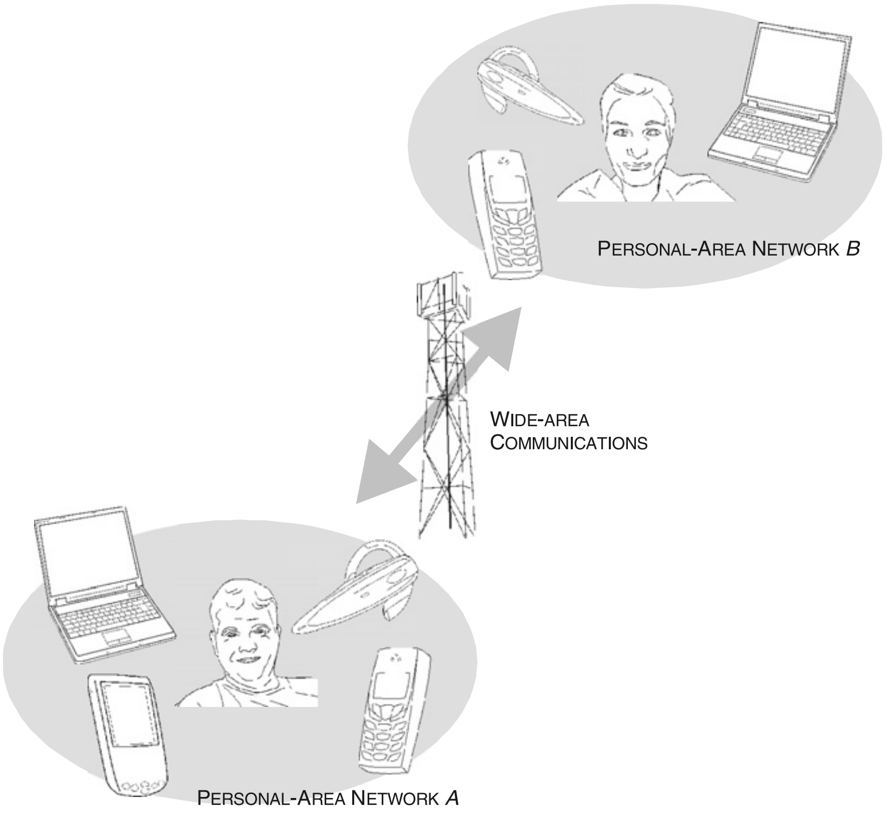


Figure 3.4 *The depiction of two personal-area networks that are capable of communicating with each other. These PANs are capable of doing so as a result of the wide-area communications network, which may be supported by a dial-up connection.*

telephone has also been with us for some time. It may be apparent to some users that a cell phone and a cordless telephone operate via a wireless medium. Nevertheless, some users (and arguably the majority of them) may only perceive the intended telephone functionality, rather than its inherent wireless capability. Although, in the United States most cellular carriers append the "wireless" reference to their brand names, such as, Cingular *Wireless* and Verizon *Wireless*. It's conceivable therefore to become familiar and complacent towards usage scenarios that depict a cell phone and a Bluetooth-enabled headset; time will tell. This essentially forms the subtle basis in our consumer perception and usage scenarios; it is this observation that distinguishes wide-area and personal-area wireless technologies.

There is nothing unfavorable with this concept, but this book primarily discusses the newer (personal-area) wireless technologies that afford a new generation of mobility and freedom. It is after all the focus of marketers to drive the new generation of wireless-enabled products, and *Developing Practical Wireless Applications* explores in some detail the existing and emerging new wireless technologies, coupled with the myriad of applications that occupy and impress upon our personal and working environments.

In the following sections we appraise the generations of more established wireless technologies and it will naturally provide a complete picture of the historical generation of wide- and personal-area, whilst molding a comparable impression of the overlap created between them. It is becoming more evident that manufacturers integrate new wireless technology into cellular phones, notebooks and so on, resulting in the overlap of wide-area and personal-area communications (see Figure 3.4). It is this overlap that bestows the mobility and freedom characteristics of our personal and working environments.

Generations of Wireless Technology

Undoubtedly, many of us have witnessed the emergence of generations of wide-area technologies each depicting the advancement of applications and digital capability. Regularly we read in the technology news, the relentless press releases announcing faster and better applications that now rely on *3G* technology (more about this later). Perhaps the label of *old* seems somewhat inappropriate, as the more established generations of the wide-area era are growing at a phenomenal rate. The depiction of wide-area communications helps us understand clearly where the respective technologies lie within the realm of personal-area emerging technologies, as we have conceptualized in Figure 3.5 (data rate vs. distance).

First Generation (1G)

First generation (or 1G) cellular telecommunications were only capable of supporting voice traffic. What's more, they were very susceptible to interference and offered no security (eavesdroppers with basic radio equipment could listen in on conversations). It has been reported that data traffic could occur, although "ideal" network conditions were required, perhaps something similar to, the wind blowing in your hair and the sun shinning on your face! 1G was introduced in the early 1980s and was based upon an analog system comprising *Frequency Modulation* (FM), *Frequency Division Duplex* (FDD) and *Frequency Division Multiple Access* (FDMA). Combining these primary methods of radio transmission and reception, several variants of the first cellular technologies emerged to include the *Advanced Mobile Phone Standard* (AMPS), *Total Access Communication System* (TACS) and the *Nordic Mobile Telephony* (NMT); these variants

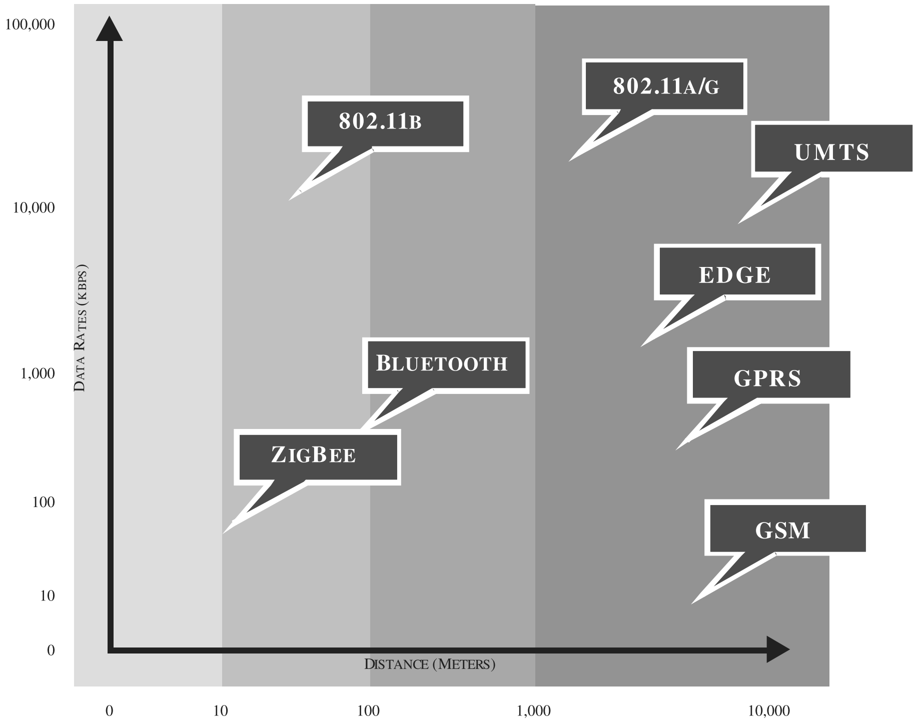


Figure 3.5 *The conceptual presentation of data rates versus distance illustrating the placement of wide- and personal-area wireless technologies.*

were widely based in North America, Japan and Europe and became the most popular and first commercially available cellular systems.

Understanding how FDMA works

FDMA offers a radio spectrum that is divided into channels, where typically each channel is 30kHz; there is also a separate control channel, which is used to manage and coordinate voice channel assignment. The reference to a channel within the FDMA rationale is in fact two 30kHz channels: one for each direction, known as *uplink* (or *reverse* channel) and *downlink* (or *forward* channel). This two-way strategy is known as FDD and typically you will come across 1G technology being referred to as FDMA/FDD. FDMA/FDD is a *narrowband* telecommunications system, which implies that the available spectrum is divided into narrow radio channels, along with a channel separator that is used to separate the uplink and downlink communication pathway (primarily to reduce the likelihood of interference). When a cellular phone initiates a call, a frequency channel is reserved for the duration of that call; frequency modulation is then used to modulate voice data within the reserved frequency band.

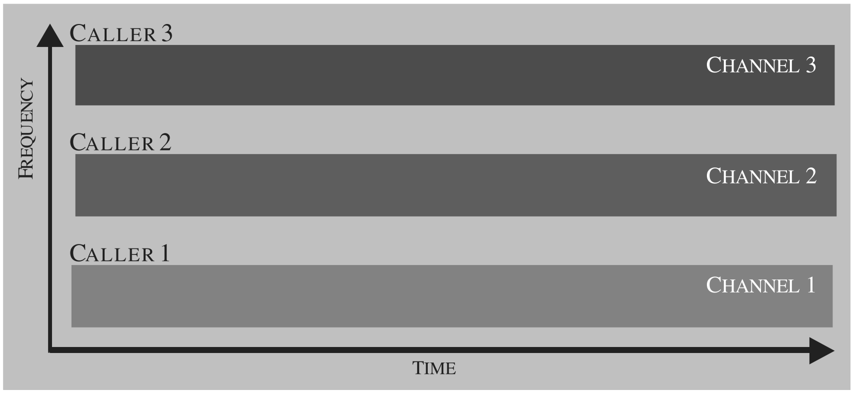
In this scenario the allocation or reservation of a channel (remember there are two 30kHz channels) is assigned uniquely to a user at any one time. Naturally, this approach limits the available number of users that can make use of the cellular service through a *base station*. A base station is a permanent erected structure that houses a transceiver and is connected to the wider telephony infrastructure, in turn, enabling the ability for a cellular user to initiate and receive calls, whilst being mobile.

This system has now been largely replaced with the digital generation of cellular telecommunications. Indeed, with the emergence of *second generation* (2G) technology, we experience a broader capability, accompanied with increased reliability and security, which now includes the ability to transmit and receive data more effectively.

Comparing analog and digital communications

It seems an endless battle of analog versus digital with the latter dominating most wireless-enabled products and, of course, most cellular-centric technologies. It is perhaps worth pausing for a moment to consider the differences and advantages that digital has over analog communication systems. An analog system lends itself naturally to the characteristics of the human voice. The signal witnessed by such a system is that of a sine wave, as shown in Figure 3.7. Unfortunately, this type of communication is prone to interference and, as such, loss of communication occurs; this sine wave represents the original format of the data being transmitted. In this particular instance, communication is highly susceptible to noise, in turn, causing unreliability (users of an analog voice-enabled system would experience noise or hissing during the conversation). An analog system also occupies a lot more spectrum, compared with its digital counterpart. Let's use our previous discussion and illustration (Figure 3.6) as an example here: the analog method (FDMA/FDD) requires two 30kHz channels,

Figure 3.6 *A conceptual representation of FDMA/FDD, where a channel is uniquely allocated to each caller (frequency vs. time).*



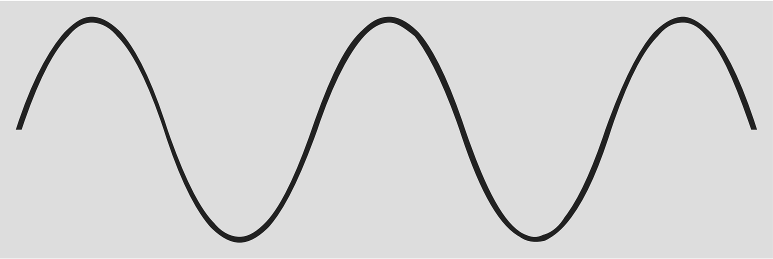


Figure 3.7
A sine wave represents the analog form of an analog-based communication system.

plus a channel separator, for the duration of the call. The bandwidth remains in use during the call and naturally this occupancy reduces the number of users who are able to use the service.

Moreover, analog communication generally remains open to eavesdroppers, as we illustrated earlier in our introduction of 1G technology. Since the analog data is transmitted in its original form various pieces of equipment, such as scanners, are available enabling individuals to eavesdrop on telephone conversations (eavesdropping is not limited to voice communication, data transmitted in this format is also prone to security risks). Additionally, analog systems consume greater power than its digital counterpart, making digital systems much more power consumption friendly.

Unlike analog, digital communication transmits its data using a series of pulses, as shown in Figure 3.8. The digital wave form has two states: high and low, which can be likened to a series of *ones* (1s) and *zeros* (0s). This representation is typical of all digital-enabled equipment. During digital transmission, a radio receiver can easily distinguish between the series of pulses (high and low) from any background interference, such as noise. Reliability is ensured using various types of encoding schemes that is added to the data transmission; if the message is not received then the transmitter will retransmit it. With the ability to digitally encode data, it's also possible to encrypt it. Using a variety of encryption methods, securing the data before transmission overcomes

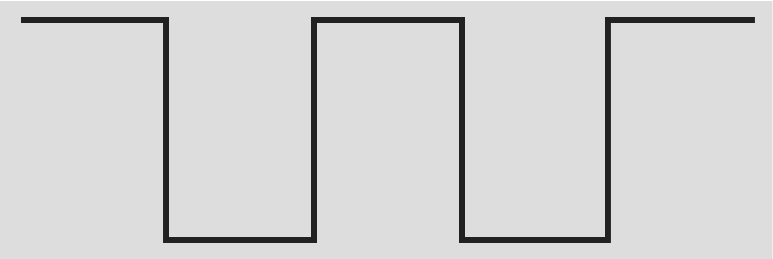


Figure 3.8
A pulse wave represents the digital form of a digital-based communication system.

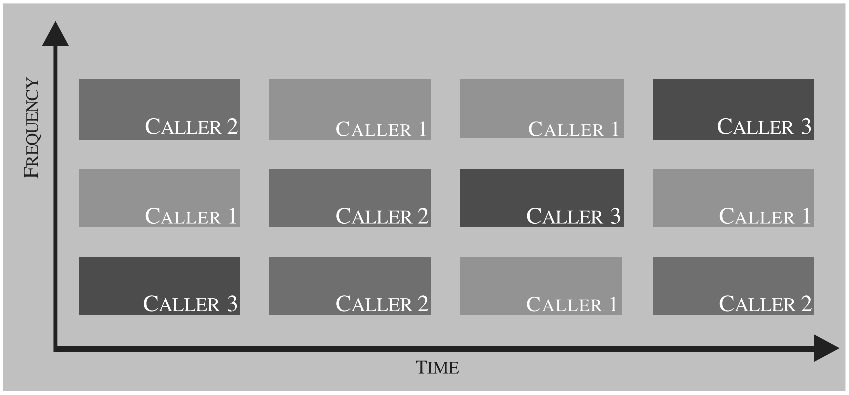
potential eavesdropping. Typically, two devices will agree upon an encryption scheme and the transmitter will decrypt it accordingly using the agreed parameters. Additionally, numerous schemes are available enabling cellular services to increase the available bandwidth; we now discuss this further in the following section.

Second Generation (2G), 2.5G and 2.75G

It is with the growth and deployment of digital capability that has led the way forward to a new set of wireless applications. Incidentally, a large part of the North American cellular coverage is still operated using AMPS (the analog system, which we introduced earlier) and, as such, US operators are actively making a shift to newer digital technologies, which we will discuss later on.

In the United Kingdom, Europe, United States and Asia several digital cellular technologies are widely used. The basic premise is the same as an analog system, in that the available frequencies that are open to an analog system are also available to a digital system. The distinction between them is that the digital system uses the frequencies in a different way, more specifically, a channel is divided into *time slots*, as we illustrate in Figure 3.9. This method is not unique to cellular communications either; similar techniques can be found in networking technologies, such as Ethernet 802.3 (a fundamental technology underlying fixed networking). The method for dividing the frequency channel into slots is called *Time Division Multiple Access* (TDMA) and there are three variants of TDMA technology currently in use: D-AMPS, *Personal Digital Cellular* (PDC) and *Global System for Mobile Communications* (GSM). These three variants are incompatible and have implemented the TDMA scheme in different ways.

Figure 3.9
A conceptual representation of FDMA/TDMA/FDD where channels are allocated uniquely to each caller (frequency vs. time).



As a result they are competitive solutions in delivering cellular telecommunication services for its consumers.

Understanding how TDMA works

TDMA offers its solution by dividing a frequency channel into time slots. It takes the existing 30kHz channel, which would be allocated to a single user for an FDMA topology, and divides it into three slots; effectively this division creates three further channels. Now multiply this over the available spectrum and you have increased the service capacity by a factor of three; however, newer TDMA systems increase this capacity by a factor of six by employing better compression techniques; in other words, compressing more data into one time slot. One of many advantages for using TDMA is its digital premise and, of course, its ability to support data-centric communications. Similarly, voice quality is increased and, as a result becomes much more secure. Other factors such as power consumption and cost effective transceivers make it an attractive option for cellular phone manufacturers.

The general strategy adopted with a TDMA-based system is known as a combined FDMA/TDMA/FDD solution and typically you will see GSM and D-AMPS referred to in this manner. TDMA digitizes the voice traffic into a packet, this is then placed into a time slot (measured in terms of milliseconds) onto a channel. For each subsequent packet a different channel is allocated, as we have already illustrated in Figure 3.9. The whole process then becomes cyclic where old time slots are reused. Control channels referred to as *Digital Control Channels* (DCCH), are also used to support call setup and control; in a similar fashion to FDMA.

Digital Advanced Mobile Phone Standard (D-AMPS)

Interim Standards known as IS-54 and IS-136 were developed and standardized by the *Electronics Industry Association* (EIA) and the *Telecommunication Industries Association* (TIA). It is these standards that govern telecommunication functionality, features and capabilities within the US (and, of course, other parts of the world where it has also been deployed) through the two systems known as AMPS and D-AMPS. It is IS-136 (an upgrade of IS-54, maintaining backward compatibility with IS-136) that prescribes digital capability for D-AMPS using the TDMA methodology. In utilizing this scheme, network operators were able to increase the number of users that could use their service by up to six times, as compared with the original analog AMPS service. Furthermore, IS-136 provides other digital features such as *Short Message Services* (SMSs) commonly referred to as *text messaging* or *texting*: a fundamental precursor to the start of the digital revolution enabling digital-based applications for cellular phones; D-AMPS typically offers a data capacity of around 9.6Kbps. It is also worth commenting that with 2.5G consumers are now capable of using *Multimedia Messaging Services* (MMSs). Currently, the ability to text enables the user to send a short text message, typically 160 characters per message, to one or more users. Some network operators provide the ability to split large text messages into two SMSs. For example, if a text message comprises 262 characters the first 160 will be sent as one text message, followed by the remainder (102 characters) as another text message. Similarly, MMS provides the ability to send text messages (with an increased capability to send larger text messages without the need to split them over one or more SMSs), but the user now has the ability to attach images, pictures and audio. Multimedia enabled cellular phones are increasingly popular with the youth market; integral digital camera capability and live video images are prevalent in the UK, Europe and Asia. It is the demand for these types of applications that are driving increased data rates, which is ultimately leading to the promised third generation technology.

Personal Digital Cellular (PDC)

PDC, also known as *Japanese Digital Cellular* (JDC), is a second generation TDMA technology mainly used throughout Japan and has some similarities to IS-136 (D-AMPS). Despite the fact that PDC is only available to Japanese consumers it still remains the second largest cellular standard in operation. PDC was developed and standardized by the *Research and Development Center for Radio Systems* (RCR) and was introduced in 1991 by NTT DoCoMo, to replace large parts of the existing analog network. NTT DoCoMo is Japan's largest network operator, which is partly owned by the Japanese Government.

The success and popularity of PDC in Japan can be credited, in part, to *i-Mode*, an Internet-based service providing capabilities such as web browsing and email. You wouldn't be wrong in thinking that this has some similarities with another technology called *Wireless Application Protocol* (or WAP) which offers comparable services. WAP was developed by a consortium of companies (Phone.com, Ericsson, Nokia and Motorola). Its aim was to establish a common platform to facilitate the presence of Internet-based applications on cellular phones. A strong argument to its development was to alleviate confusion for the consumer, since there are numerous telephony standards for delivering cellular telecommunications, namely D-AMPS, GSM, PDC and so on. It would be natural to assume that a crossover, from PCs to cellular phones and its web-based applications would begin to emerge. However, with the intrinsic small screen area it was all too often cumbersome and awkward to navigate. *Internet Service Providers* (ISPs) had to rewrite areas of their website to enable users of WAP-enabled phones to view web pages and, as such, a large business community had to invest effort and expense in realizing the WAP dream. The offer of WAP Internet-based services didn't mature in the direction that network operators had hoped and established only poor to moderate success.

i-Mode on the other hand established over six million subscribers (circa 2000) by operating a technology that was not compatible with WAP. It's estimated that today i-Mode has over forty million subscribers in Japan and an increasing user base in the rest of the world (i-Mode is provided to numerous network operations in Europe and Asia). NTT DoCoMo's decision not to use WAP and instead deploy a modified version of the *Hypertext Markup Language* (HTML) called *Compact* HTML (C-HTML), as well as, utilizing several proprietary protocols proved to be judicious. In other words, combining the existing wealth of Internet-based protocols with an effective marketing model guaranteed i-Mode's world-wide popularity.

Global System for Mobile Communications (GSM)

GSM is the most popular second generation cellular standard in the world and started its life in the 1980s. It has been deployed throughout Europe, as a de facto European standard, and the rest of the world, to include South America, Australia, Asia, the Middle East and Africa). In the US, D-AMPS is being superseded by GSM and other world-wide deployments of the technology will also be gradually phased out. At the time of writing, current figures estimate almost two billion consumers spaced over approximately 200 countries use GSM as their cellular service. Additionally, it was the first cellular system to specify digital capability and define network infrastructures. The standard is governed by the *European Technical Standards Institute* (ETSI), who undertook the responsibility in the early 1990s. With the introduction of GSM as a de facto European standard, operating at 900MHz and 1800MHz (whereas North America utilizes the 1900MHz band), we have begun to establish a globally reliable and effective system for telecommunications.

With the continued growth and demand for better applications, that is, applications beyond voice capability, GSM has evolved accordingly. A fundamental prerequisite of any telephony service is the ability to deliver high-quality voice traffic. And it is fair to comment that this has been successfully established, tried and tested where many consumers benefit form this core service. Network operators continually seek newer value-added services that will attract various consumers to their network, services and products. Operators offer data-centric services that build up on the already established core application; in its many guises we may have witnessed this evolvement as 2.5G and 2.75G; an empirical advancement towards third generation technology. Second generation technologies (D-AMPS, GSM and PDC) offer very basic levels of data connectivity where throughput varies from 9.6Kbps to 14.4Kbps. To deliver effective data-centric services an increase in data throughput and a reliable medium needs to be provided. GSM has established itself as a successful technology and has witnessed a series of *extensions* or *upgrades*. In the following sections we identify some of the extensions that are in operation today enabling faster data throughput for our demanding applications. These extensions typically surround GSM, after all it is the most popular telecommunications technology in operation today. Modifications to the GSM standard comprise a number of steps along the path to third generation and are typically characterized as 2.5G and 2.75G.

High-Speed Circuit Switched Data (HSCSD)

ETSI first commercially released *High-Speed Circuit Switched Data* (HSCSD) in 2000 and is the first of many upgrades to GSM. It's not common to see HSCSD placed into a category of cellular generations, but typically we would see it being placed into 2.5G.

Circuit Switched Data (CSD) is very much characteristic of a *Public Switched Telephone Network* (PSTN). A user will make a call and the telephone network will direct (or switch) the call to the destination through a series of circuits whilst adopting an economical perspective. In other words, it will make the least number of steps to get to its destination. Once a connection is established the circuits essentially create a *dedicated* pathway between source and destination. This pathway does not change nor can it be used by any other caller for the duration of the call.

GSM inherently offers data throughput of up to 9.6Kbps and mandates error control in transmission ensuring high-quality voice reception. This is achieved in the same way that voice traffic is digitized and then placed into a time slot; data is also allocated into time slots. HSCSD is capable of offering data speeds of up to (approximately) 57.6Kbps, which is comparable with most analog modems. It achieves this throughput by taking advantage of the available time slots used within the TDMA scheme. Instead of using one time slot, as it does for voice, it uses and reserves multiple time slots (a maximum of four) during a data-centric connection. Additionally, HSCSD eases the error control mechanisms imposed by the GSM standard and therefore increases data throughput up to 14.4Kbps per slot. Obviously, this will reduce the available number of slots for consumers making use of the voice service. With this scheme and the potential reduced capacity, operators charge the user for the duration and number of time slots occupied.

General Packet Radio Service (GPRS)

The first notable upgrade to characterize the evolution of cellular communications was through the introduction of *General Packet Radio Service* (or GPRS). With this introduction the general telecommunications community acknowledged that we had achieved one significant step in the evolutionary cellular generation scale. Essentially, with GPRS we are at 2.5G; a true indicator that we are moving towards a better cellular communications experience.

GPRS differs to HSCSD in that it utilizes a *packet-switched* scheme. CSD uses a series of circuits which remain unavailable during its use. GPRS, on the other hand, uses the same packet transmission scheme that underlies the Internet. In comparison, HSCSD creates a dedicated pathway and GPRS sustains a *connectionless* topology. A connectionless network allows users to enjoy a shared bandwidth in the same manner that the Internet does. Data packets are transmitted using time slots that are freely available, although in reality GPRS defines a set of classes, which mandate numerous transmission schemes. A particular class scheme will reserve upload and download time slots for low to high data transmission; each class would have varied throughput, but operators would charge accordingly for higher data rates. Typically, users would experience a data rate of between 57.6Kbps and 171Kbps. GPRS was introduced with the primary objective to establish a much more efficient and cost effective solution for the user, in turn, enabling reliable data-centric applications. GPRS allows users to have an always-on presence, as operator charges only apply to data that is actually transmitted and received over the network.

Furthermore, WAP has enjoyed an increasing success, as the data rates offered through a GPRS connection are greater than the standard GSM offering (9.6Kbps). Similarly, the GPRS introduction has inspired and infused many ISPs to modify some of their web space to reflect WAP users. The interface is still basic, but is becoming increasingly intuitive and popular with today's users of *SmartPhones*.

Enhanced Data Rates for GSM Evolution (EDGE)

With a continued need for faster data throughput coupled with the emergence of multimedia and video-based applications and, of course, the advancement towards third generation technology, *Enhanced Data Rates for GSM Evolution* (or EDGE) was introduced in 2001 and is characterized as 2.75G.

EDGE relies upon the TDMA time slot scheme, but varies the scheme by using a different modulation technique. *Gaussian Minimum Shift Keying* (GMSK) is the modulation technique used for GSM, which evolved from other simpler schemes. EDGE uses an *8 Phase Shift Key* (8PSK) modulation technique, where it aims to achieve data rates of up to 384Kbps utilizing the packet-based like delivery of GPRS. Essentially, this new modulation technique compresses and squeezes so much more into one time slot; remember we started with GSM merely offering us 9.6Kbps. At the time of writing EDGE is very much prevalent in North America and in contrast, operators are contemplating skipping this mid-generation technology and heading straight towards third generation implementations in the majority of Europe.

The premise of these modifications, including HSCSD and GPRS, utilize the facilities already available with an existing network infrastructure. Ultimately, this infrastructure cannot endure changes to it on a regular basis; as a result we see architects modify or tweak the existing technology supported by the network. A deployment of established *base stations* (more about this later) on a national scale would surely translate into an overwhelming unwillingness for operators to upgrade the associated hardware. Naturally, making regular modifications incurs cost and would perhaps stagnate the advance of telecommunications. Some upgrades typically occur at a software level; for example, we can upgrade a piece of software on our notebook or cellular phone, so too can operators systematically upgrade their collection of stations with the ease of pushing a button. Despite these innate reservations some modifications have to be made at the hardware level, primarily to accommodate the encoding and decoding of the 8PSK scheme. Evidentially, we may be witnessing the reason behind European operators' unwillingness to move in this particular direction. Hardware modifications don't stop there either, cellular phone technology also needs to be updated with new 8PSK ability. This burden isn't too hard to accommodate, as manufacturers are constantly improving cellular phones.

Cellular roaming

With a good foundation upon which we can enjoy reliable voice and data services, we need to understand how collectively these technologies are brought together, after all we take these capabilities for granted and are able to use them no matter where we are in the world.

We introduced in our earlier section the notion of base stations. These units are distributed geographically and when we receive or make a call, the cellular terminal connects with its registered base station. The ability to roam from city to city is provided by a series of base stations that are strategically placed in proximity with each other. As the cellular user moves to the edge of coverage provided by one station (viewed as a cell, see Figure 3.10), the cellular phone, will automatically handover to the next available station. Network service providers will distribute base stations to create an optimum operating environment. Factors such as buildings, hills, mountains, valleys, the weather and so on, as well as potential interference that may be caused by the base stations themselves, are issues that are taken into consideration. As a result, this technology enables cellular users to take their cell phone across several states and across the world allowing them to utilize the telephony service of a particular state or country; this is of course subject to the user having *tri-band* support within their cellular phone. A cellular phone that has tri-band support is capable of operating in the three network bands (900MHz, 1800MHz and 1900MHz) offered through GSM.

Third Generation (3G)

The rate at which new telecommunication standards are being developed is phenomenal. Alongside the introduction of HSCSD, GPRS and EDGE as standard methods

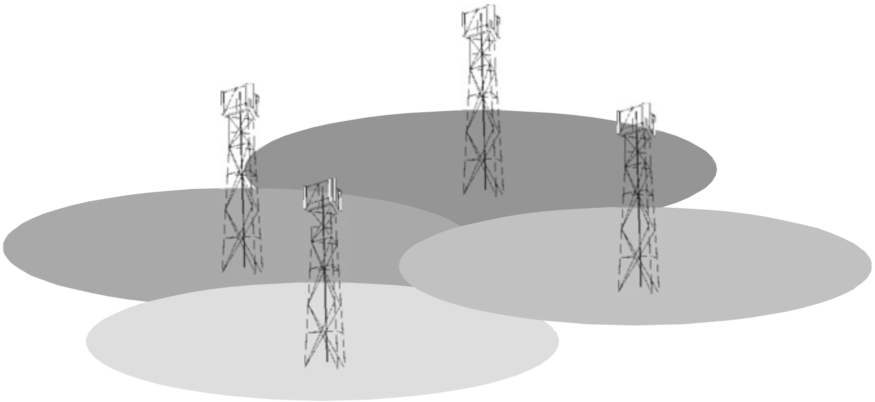


Figure 3.10 *The cell-like infrastructure that is provided by a collection of base stations strategically distributed over a large area. These areas may range from hundreds of meters to thousands of meters, depending upon the optimum operating environment.*

of data connectivity, operators are eager to deliver advanced methods for data-centric applications, such as broadcast quality video. Remember, we can already rely on voice and, to an extent, data connectivity. Operators are always keen to create new scenarios where there is an increased and continued revenue stream. To that extent, in 1998 the *Third Generation Partnership Project* (3GPP) a collaboration of partners, which comprise a number of standards bodies, such as ETSI, the *Telecommunications Technology Committee* (TIC) and the *Association of Radio Industries and Businesses* (ARIB) to name but a few, made a consorted agreement. The primary objective of this group is to maintain and support the existing cellular infrastructure and associated technologies (that is, GSM, HSCSD, GPRS and EDGE). The scope of these activities also extends to specifying new standards for third generation technology. This will ultimately benefit the operator, as there is a united driving force ensuring high-speed interoperable telecommunications standards.

Within the 3G arena an additional multiplexing technique is used called *Code Division Multiple Access* (CDMA). This forms our third multiplexing scheme where our two previous methods were FDMA and TDMA. CDMA is a *direct sequence* (DS) technology utilizing a spread spectrum topology where multiple users occupy the radio channel and frequency concurrently (we will discuss this in more detail later). An exception to the appearance of CDMA within 3G is *cdmaOne*; it's widely deployed in the US and Korea and is classified as a second generation technology. It is defined by IS-95 and is now superseded by IS-2000 (also called CDMA2000) and is very much in competition with GSM. CDMA was initially developed by Qualcomm (www.qualcomm.com) a research and development company based in the US.

Table 3.1 *The range of derivative CDMA technologies, which are not necessarily interoperable*

Name	Description
CDMA	With numerous variants of the CDMA standard; *CDMA* itself can be used as a collective noun.
cdmaOne	The initial generation of CDMA (2G) which is defined by IS-95 and is used predominately in the US and Korea.
CDMA2000	IS-2000 is a superset of IS-95 (3G evolution).
WCDMA	Initially developed by NTT DoCoMo and now used to form the basis of UMTS, it is a key third generation cellular standard.
TD-SCDMA	A standard that is set to become widely adopted in China and therefore not dependent upon other developed cellular standards.

One other CDMA variant includes *Universal Mobile Telecommunications Service* (UMTS) which is based upon *Wideband* CDMA (WCDMA); this is perceived as third generation. 3GPP's activities are concerned with defining UMTS. More confusingly, there is a second group called the *Third Generation Partnership Project 2* (3GPP2) whose activities include defining third generation technology evolved from CDMA2000. cdmaOne, CDMA2000 and WCDMA are incompatible standards and are summarized in Table 3.1.

WCDMA was developed by NTT DoCoMo as Japan's third generation *Freedom of Mobile Multimedia Access* (FOMA) technology. This became the initial draft of UMTS after NTT DoCoMo submitted it to the *International Telecommunications Union* (ITU). ITU, a global standards body, adopted and subsequently incorporated WCDMA into its *International Mobile Telecommunications-2000* (or IMT-2000) specification. This specification is pivotal in identifying key attributes of what characterizes third generation cellular technology. One glowing characteristic of the IMT-2000 specification is the attempt to bring together a cohesive cellular experience where world-wide cellular infrastructures interwork and interoperate. This translates into users being capable of utilizing one cellular phone and moving it from state to state and country to country with transparency and ease. The ITU, 3GPP, 3GPP2 and the *Universal Wireless Communications Consortium* (UWCC) all work in partnership to realize IMT-2000. In addition to providing cohesion, the IMT-2000 also defines the increasing need to deliver broader applications to include a range of multimedia services from a single cellular platform. Numerous data rates are offered for a number of application contexts where a minimum of 2Mbps for cellular users, in a fixed location is offered, to lower data rates (of 384Kbps and 144Kbps) for mobile consumers, such as pedestrians and vehicle connectivity.

The Republic of China has also made its own contribution to the IMT-2000 partnership in association with Siemens. It has defined a CDMA derivative called *Time Division Synchronous* CDMA (or TD-SCDMA) and was incorporated by the 3GPP in 2001 as part of the UMTS standard. It is envisioned that TD-SCDMA will initially be deployed in China where, at the time of writing, field testing is being conducted. Underlying UMTS is a radio access method called *Universal Terrestrial Radio Access* (UTRA), which constitutes the WCDMA, UTRA/FDD method and the TD-SCDMA, UTRA/TDD (*Time Division Duplex*) method. The two methods offer complementary mechanisms each accommodating the various services that are available through UMTS.

Understanding how CDMA works

CDMA is a *Direct Sequence Spread Spectrum* (DSSS) technology that doesn't transmit on a particular frequency, as compared with FDMA and TDMA. Instead, it uses all the available bandwidth for multiple users in the same channel, where *codes* are assigned to identify individual connections. We illustrate the conceptual model of CDMA in Figure 3.11. Despite multiple users using the same channel no interference occurs between conversations. Like FDMA and TDMA, CDMA has access to the same spectrum, but merely alters the way it uses that spectrum. It is the unique characteristics of the spread spectrum technique that makes this possible. In short, data is transmitted in its rawest form (binary 1s and 0s) and is spread over a channel in a pseudo-random pattern. Both the transmitter and receiver have agreed how to pseudo-randomly encode and decode the binary data. Similarly, with a number of potential callers engaged in a connection, a receiver will only listen to a particular conversation, that is, the conversation that has the right code.

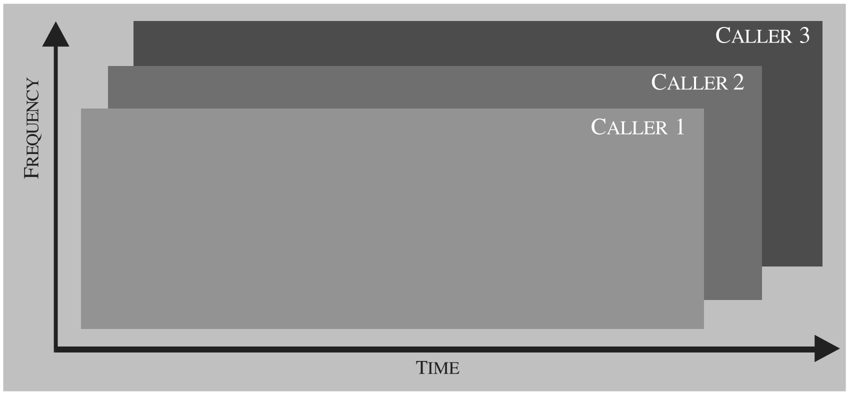


Figure 3.11 *A conceptual representation of CDMA where the spread spectrum technique enables multiple users to use the same channel without interference.*

The next generation of cellular applications

Will we see the emergence of fourth generation (4G) technology? Yes, we will, and arguably most academics, researchers, and cellular advocates believe it's already here, but it's a matter of timing and belief. Japan is directing considerable effort in research and development for this "fourth generation" technology. It is unclear at this stage what is meant by 4G; how it will be constituted and so on. Several companies believe that the technology will simply be an upgrade to 3G and others believe it will completely replace the existing infrastructure. The latter belief is somewhat difficult to understand, as so many companies have invested so much into delivering 3G technology. The proposed shift from 3G to 4G is beginning to take shape, albeit on a visionary basis only, as operators are in the process of deploying 3G cellular services. For example, within the United Kingdom several operators have only recently introduced 3G services for its consumer base. Again, it's hard to understand why operators and the like would want to replace their existing infrastructure. We will inevitably witness 4G or at least the concept of this technology, delivering full broadcast quality television across a cellular network; this effort forms part of the R&D currently undertaken by the Japanese companies. Perhaps 4G will only exist as a concept, but its emergence as a full-bodied deployment, most certainly on a national basis, is still a long way off. Increasingly, with an eagerness to create better wireless applications, perhaps the emergence of 4G technology will itself exist as an amalgamation of wireless technologies, in turn, creating *wireless convergence*.

Wireless Convergence

Wireless *convergence* is a relatively new term which unites personal- and wide-area communications into a single solution and, indeed, it may describe itself as the new fourth generation. It is the convergence of these technologies into a single product that provides a consumer with numerous methods of connectivity. We should also differentiate convergence and *coexistence*, as these describe two very different characteristics. In the early days of Bluetooth technology and the domination of 802.11b, as a wireless networking solution, many (press and manufacturers alike) argued that these technologies could not cohabit. Furthermore, many claims were made that other external factors, such as microwave ovens, would also affect the operation of these technologies. In short, coexistence refers to the operation of two technologies that use similar radio spectrums to deliver wireless applications; both Bluetooth and 802.11b use the unlicensed spectrum 2.4GHz. Currently, as we see the emergence of ZigBee (also using the 2.4GHz radio spectrum) similar questions are being asked surrounding the coexistence with 802.11b and Bluetooth. Nonetheless, we are assured that the 802.15.4 standard, which defines the *physical* (PHY) and *Medium Access Control* (MAC) layers of ZigBee, will overcome any obvious shortcomings. We discuss the characteristics of ZigBee in Chapter 12, *ZigBee: Untethered and Unlicensed*. Similarly, with the Specification of the Bluetooth System: Core v2.0, *Enhanced Data Rate* (EDR), accompanied with *Adaptive Frequency Hopping* (AFH), we will see a more harmonious uniting of Bluetooth and 802.11b and other technologies using similar spectrums.

With such an array of wide-area communication technologies we can be forgiven if we are unable to recall that we're just using a cellular phone. Do consumers really need to know how it works? No. Although, manufacturers are keen to tell us that the latest phone uses Bluetooth – "a new generation of technology that doesn't use cables." Of course it hasn't escaped you that we were already using a technology that is cable-less.

Many manufacturers are considering integrating many personal-area technologies into the cellular phone. We have already come to expect *Infrared* (IrDA) and Bluetooth as standard personal-area technologies, but some manufacturers are also considering integrating WiFi (and in fact have already done so). One fundamental reason is to enable users to access the Internet at a competitive price, compared with HSCSD and GPRS. Some other applications may include *Voice over Internet Protocol* (or VoIP) – naturally, these two applications will require the presence of a *hotspot* (as we illustrated in our anecdote within Chapter 2, *Understanding the Wireless Audience*). With the ability to utilize services and having the support of data connectivity across a cellular network, home and business users alike will be capable of connecting to a number of ISPs, in turn, allowing them to view web pages from the Internet or office Intranet. Similarly, users will also be able to send and receive emails. This traditional method of connectivity is being largely replaced with the appearance of hotspots and, more recently, with the potential of *Worldwide Interoperability for Microwave Access* (WiMAX), more about this later. It is predicted that with such an intense population of wireless hotspots, the need to utilize a dial-up connection will seem somewhat primitive. It should go without saying that these two applications won't please many carriers as it conflicts with their core revenue stream – income from data connectivity and voice traffic.

Perhaps manufacturers should focus on complementary technologies such as IrDA and Bluetooth. The former is a tried and trusted technology that enables users to synchronize and transfer files between a notebook and a phone. Bluetooth is becoming more and more trusted and a reliable medium upon which consumers can achieve similar functionality. Indeed, users of Bluetooth-enabled cellular phones now come to expect headset operation as a standard feature. However, *Near Field Communications* (NFC) is set to become a new technology that will add other complementary features to your phone. The NFC standard was approved by the *International Organization for Standardization* (ISO) and the *International Electrotechnical Commission* (IEC) late 2003 and was co-developed by Sony and Royal Philips Electronics. The standardization process realizes true compatibility and interoperation of NFC-enabled devices and, as such, Nokia, Sony and Royal Philips Electronics launched the NFC Forum (www.nfc-forum.org) in March 2004.

NTT DoCoMo introduced Sony's *Felica*, a wireless payment and ticketing system, in August 2004, which uses NFC technology. Similarly, Royal Philips Electronics has developed *Mifare*, which is interoperable with Sony's Felica product. Primarily, Felica is a wireless smart card system that allows users to purchase shopping, cinema tickets and so on, using a cellular phone. The name Felica is derived from the word "felicity" meaning happiness or contentment, although equally, watching Felicity Kendal in *The Good Life* (BBC) also creates an unmeasured sense of contentment. This whole concept isn't entirely new, but it's only now that we've seen it emerge onto the marketplace. When consumers reach the check-out point, payment can be made by passing the cellular phone across a wireless smart card reader; this notion is very similar to the *e-wallet* concept. The range of applications doesn't stop there either. Wireless entry systems, such as *e-logging* provide users with the ability to enter buildings or to log on to a computer wirelessly. Again, the user would pass the cellular phone across the wireless reader. It is also envisaged that cellular phones will be used as a wireless entry system for your car and to start the engine.

NFC has an operating range of 5cm (1.97in) or 10cm (3.94in), although some manufacturers are extending this range for a host of other new applications, such as personal audio entertainment. It uses magnetic induction to transmit data from one device to another and inherently provides secure and reliable transactions. It's inherently secure because of the limited range, and malicious intent should be obvious. It mandates a peer-to-peer topology and is complementary to Bluetooth and WiFi. One such application in this particular context is to utilize NFC over Bluetooth and WiFi to enable hassle-free connectivity. With this particular application, users would no longer have to define parameters required to set-up a Bluetooth or a WiFi connection, as NFC would intelligently exchange the configuration parameters for you.

Wireless convergence fulfils part of a wireless trend that ultimately provides a holistic range of applications that provide consumers with multiple choice options for connectivity, perpetuating the notion of mobility and freedom. With an appropriate balance of consumer demand and wireless availability we can surely achieve a sense of reality in all our day-to-day expectations.

Broadband wireless

WiMAX is set to create an opportunity for permanent connectivity for users on the move or in the business and home. It essentially forms a hotspot that covers a radius of 10km (6 miles). The WiMAX Forum (www.wimaxforum.org) is an organization that mandates the interoperation and deployment of *broadband wireless access* (BWA), where a consortium of companies, including Intel, comprises this non-profit organization. The 802.16 standard is mandated by the IEEE and ensures compliant delivery to market of broadband wireless equipment.

WiMAX is a technology that interconnects *Wireless Local Area Networks* (WLANs) or WiFi hotspots, whose backbone is connected to the Internet. It forms part of a *Metropolitan Area Network* (MAN) that enables *last mile* connectivity for consumers by extending the fixed infrastructure over a short distance. More specifically, to deploy a cabled infrastructure for homes and offices can be an economical burden for telecommunication providers and WiMAX is perceived to deliver connectivity for a number of homes and businesses more cost effectively. It promises to deliver a shared bandwidth of up to 70Mbps over distances of 10km (6 miles); we are assured that the bandwidth would be sufficient to meet the requirements of up to sixty businesses and a thousand homes. With this level and potential range of connectivity we begin to blur the boundaries that exist for personal- and wide-area communications.

Manufacturers' Refocus of Consumer Perception and Usage Models

Wide-area communication is evolving and emerging with new standards but nowadays its focus is directed towards added-value and improved services and applications. Essentially, cellular operators are certainly confident that at its core a cellular phone will allow you to make and receive voice and data calls. But hitherto, there is an emergence of products that enable you to use a host of flexible applications, combining and extending the notion of mobility. Personal-area wireless technology focuses on the ability to be mobile and free from the constraints of a fixed environment. Essentially, personal- and wide-area technologies have bestowed users with a sense of freedom and, with time, we will artlessly reach an extent where we will secure familiarity in the knowledge that its existence will inexplicably be taken for granted.

An endless introduction of personal-area communication technology, each announcing a new definition of life-style, and all of which is emphatically endorsed by a team of marketers indoctrinating the notion that your life doesn't exist without it, perhaps prematurely, pushes the technology into the top drawer of uselessness. As visionaries, engineers, marketers, investors and laymen we need to ensure the direction of wireless technology justifies a particular need that, in turn, becomes well suited to meet the expectations of the consumers who indirectly determine its longevity.

Who is in the driving seat of the new technology revolution? Do we have a team of marketers who dream the wonderful dream, lacking insight into the nature of what drives consumerism, accompanied with an unguided and untested stream of expectations? Or perhaps, do we have a team of techno-geeks, riding a wave of techie-ness claiming that this all new signing-and-dancing gadget will undoubtedly revolutionize someone's life? Let's hope that this dichotomy of expectation and needs converge to ultimately guide the revolution.

Summary

- Wireless communications as a transport medium has enabled electronic devices to exchange data wirelessly, transparently and effortlessly.
- It wasn't until the 1940s that we saw the emergence of commercial digital wireless and cellular technology.
- Wide-area and personal-area communications share a common radio medium in which data is transferred between electronic devices.
- Consumer perception and usage scenarios distinguish wide- and personal-area technologies.
- Cellular and satellite communication are tried and trusted technologies that have been around for many years.
- We've come to know wide-area communications as telecommunications.
- With telecommunications, users have been able to establish a level of familiarity where the wireless capability is no longer the perceived application.
- New wireless technology focuses on the development of personal-area communications.
- Bluetooth, WiFi, WiMAX and so on, afford the user greater flexibility in their personal and/or working environment.
- Personal-area technology allows users to create their own personal communications environment.
- Wide- and personal-area communications may overlap, where the combination of each environment allows the user to exchange data over distance.
- One distinction that can be made between wide- and personal-area is familiarity.
- Users no longer perceive a cell phone as a wireless-enabled product.
- This notion holds true for the cordless telephone.
- Users may only perceive the intended telephone functionality, rather than its inherent wireless capability.
- In time we will see users adopting the same familiarity with a cell phone and a Bluetooth-enabled headset, for example.

- There has been an emergence of generations of wide-area technologies each depicting the advancement of applications and digital capability.
- The generation of telecommunications started with 1G and has evolved to 2G, 2.75G and 3G.
- Many companies are sketching out 4G, but it's still unclear what this will actually mean.
- Some argue that 4G will in fact become wireless convergence, the amalgamation of personal-area and wide-area technologies.
- Companies are striving to achieve added-value and improved services and applications.
- A new host of wide-area applications will emerge extending the notion of mobility.
- Personal-area focuses on the ability to be mobile and free from the constraints of a fixed environment.
- We need to ensure that the direction of wireless technology justifies a particular need that, in turn, becomes well suited to meet the expectations of the consumers.
- We need to question who is in the driving seat of the new technology revolution.
- A combination of "marketers and techno-geeks" will ultimately guide the revolution.

4

Can we Confidently Rely on Wireless Communication?

Many books have been dedicated to the security of wireless technology and a number of reports have sensationalized security breaches, deeming the technology insecure and, subsequently, ineffective. The collective technology press seems to revel and bathe in the failure of our endeavors. Similarly, this particular breed of journalist observes passionately, as the wireless visage of solidarity from manufacturers, engineers and developers begins to dampen in light of the media-perpetuated public's fear surrounding wireless security. The consumers who want "out of the box" solutions are the ones who will experience a new wireless product's security inadequacies first-hand. Although, due to its innate invisibility, they may not realize this until it's too late – the damage has already been done. The technologists, who are constantly striving to simplify usage models and usability for everyday users, will then find themselves inevitably making excuses to the media as to why the security of a particular wireless product isn't exactly as watertight as expected. Sadly this only serves to further intensify our fears and prolong journalists' narcissism. Security is crucial to the success and future of wireless technology; users and companies need to be confident that their data is secure. It should therefore become an inherent procedure for manufacturers to help and educate consumers and, likewise, for businesses to establish safer and more secure infrastructures.

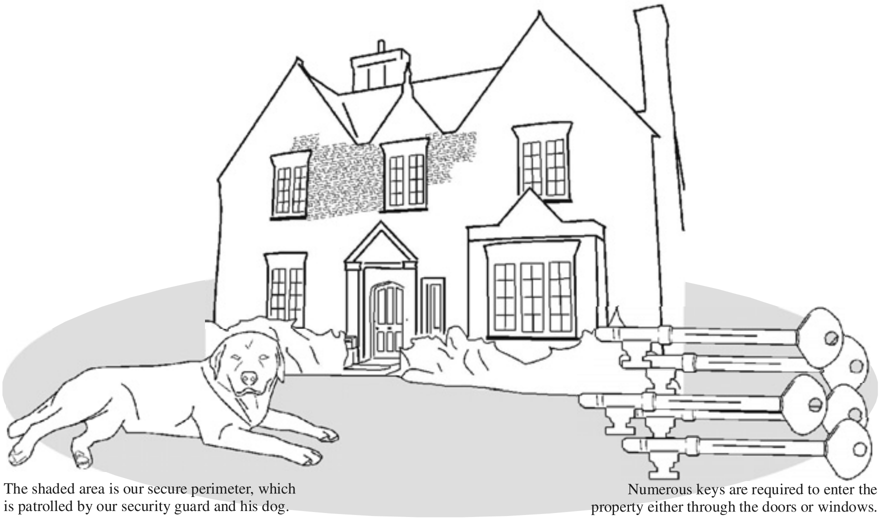
In this chapter we explore the failures and successes of wireless technology by examining how secure wireless technology really is and, similarly, how secure it is becoming? With recent reports of (now take a deep breath) *War-Driving, War-Walking, War-Flying, Phishing*, *BlueJacking* and *BlueSnarfing*, can we be certain that our wireless networks and their stored data are secure? This chapter also considers the security aspects that are currently in place and examines how best they can be improved. Wireless technology is here to stay and, in recognition of this, we will draw upon specific implementations and review a number of security architectures that aim to be the building blocks of a secure infrastructure. We may indeed become resolute regarding a technology's sustainability but we must continually question its potential success through adoption by the greater masses. Additionally, we will consider aspects of coexistence and interoperability, as these mechanisms assure us of a harmonious user experience. With personal-area wireless emerging and being integrated into commonplace products such as the cellular phone, we are indeed becoming increasingly aware of a need to connect to a variety of service providers transparently.

There is no denying it; we have all, in some shape or form, come into contact with wireless technology. And, for the agnostics among us, you should take a moment to consider whether you have recently come into contact with an infrared (TV remote control) device or a cellular/cordless phone? With the continually growing awareness and increasing familiarity of technology we can sometimes forget the mechanics underlying a product. Its phenomenal growth has captured the imagination of users and businesses alike and we can now witness WiFi in homes and offices around the globe, as well as seeing a combination of WiFi and Bluetooth technology incorporated into notebooks and cellular phones as a standard method of connectivity. In some instances we may have witnessed this technology superseding infrared. Incidentally, we have touched upon standards-based technologies; there are, of course, numerous proprietary wireless technologies serving us in some way. Take a closer look around you; for example, next time you're in a restaurant you may be offered a handheld payment device at the end of your meal. Moreover, cellular operators are now integrating WiFi into cellular phones to enable a further set of, yet to be defined, applications. Similarly, ZigBee and *Ultra-Wideband* (UWB) are relative newcomers to the industry and each has an opportunity to start as they mean to go on. In other words, it is absolutely critical that these fresh-faced and often pimple-ridden technologies establish a sensible security ethos, as to assure their future success. Similarly, with the recent alliance of the Bluetooth *Special Interest Group* (SIG) and UWB; UWB will undoubtedly inherit all of Bluetooth's security features, as Bluetooth evolves into a more secure technology (see Chapter 11, *Bluetooth: A Cable Replacement Technology*).

How Safe is Your House?

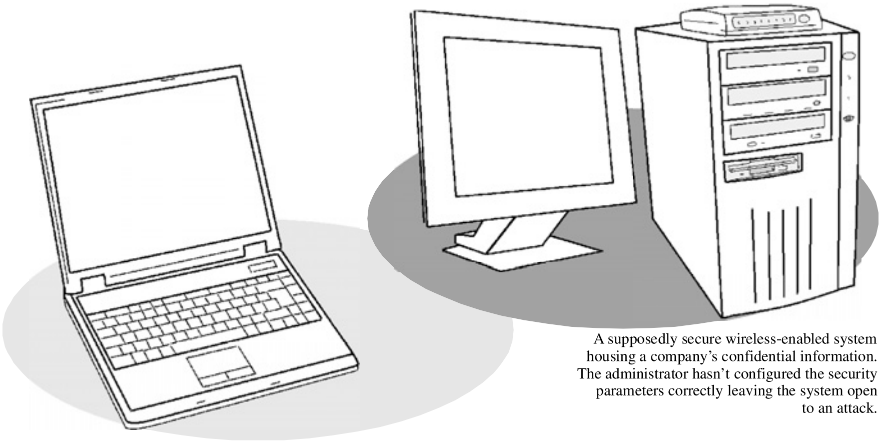
We will start our exploration of wireless security by returning to some fundamentals. These techniques are not necessarily exclusive to wireless and we can certainly observe many parallels with existing fixed networking environments. The architecture of wireless security can be likened to the requirement of a secure home – that is, securing its contents, its perimeter and surrounding grounds. We establish that our valuable possessions are placed into a safe, which requires a security code to access it; locks are required to eliminate the possibility of unwanted individuals entering our house and, as such, front and rear doors of our property are secured with locking mechanisms. Not content with placing locks on our doors, we also secure our windows with additional locking mechanisms. Nevertheless, there are still weaknesses in our secure home. Our locked doors and windows may become compromised as they can be forcibly opened, but with the availability of a security alarm we can help further deter unauthorized access. When a door or window is breached an audible warning alerts the authorities and assistance is provided. Let us take this to another level, where your home occupies a secure perimeter; the property boundary is patrolled by a security enforcement officer (and his dog). Anyone attempting to breach this secure area is challenged and, incidentally, in Figure 4.1 we depict this scenario.

In establishing this analogy we can begin to formulate parallel security procedures that can be inferred from wireless (or fixed) technology. Let's begin with the security officer that patrols the boundary: the officer will challenge any individual attempting to approach the secure perimeter. However, we know with wireless technology that the radio coverage may exceed the boundary perimeter and, as such, potential eavesdroppers may attempt to listen in on the ensuing communication some distance from the building. In Figure 4.2 we illustrate the basic equipment and tools that a hacker may utilize to gain unauthorized access to your network. In a similar vein, any individual attempting to access a secure wireless network will be challenged by the host (or server). Like the host of a computer network, the security officer will request identification ultimately to determine if you're an authorized user; the host


The shaded area is our secure perimeter, which is patrolled by our security guard and his dog.

Numerous keys are required to enter the property either through the doors or windows.

Figure 4.1
In discussing some security fundamentals, we can liken our wireless security ethics to some household principles.



A supposedly secure wireless-enabled system housing a company's confidential information. The administrator hasn't configured the security parameters correctly leaving the system open to an attack.

A keen hacker uses minimal equipment to gain unauthorized access to confidential information; suitably equipped with a wireless laptop and wireless sniffer the hacker can eavesdrop on any conversation.

Figure 4.2
A hacker will use basic equipment and tools to gain unauthorized access to confidential information; s/he may use a laptop with a wireless-enabled client and wireless sniffer to eavesdrop on any conversation.

will request that you supply a username and password to successfully enable you to gain access to the wireless network. We can refer to this process as *access control*. In other contexts, some service providers may offer a free Internet connection where anyone with a wireless-enabled device can access the Internet for free. In this particular instance, administrators would naturally protect the backbone infrastructure of their network.

Access Control

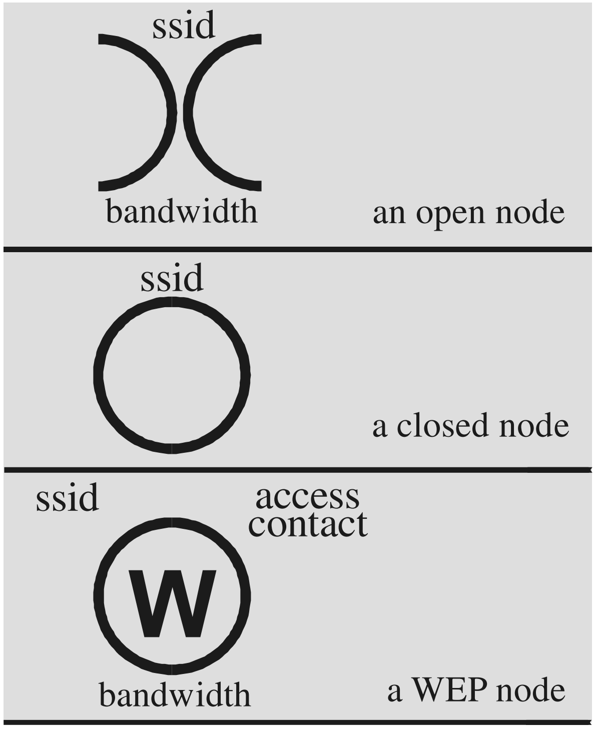
In short, access control refers to the means by which a user can successfully gain access to a service, which is available through a wireless (or fixed) *Local Area Network* (LAN) or *Wide Area Network* (WAN). Numerous methods are used to ensure that you are an authorized user. For example, *Remote Authentication Dial-in User Service* (RADIUS) is a de facto industry standard protocol, which is used to verify users of a particular service through a centralized database such as a *Network Access Server* (NAS); usernames and passwords are crosschecked with the database to ensure that the user is authorized. A NAS may include a *Virtual Private Network* (VPN) or a wireless *Access Point* (AP), but typically, in a larger organization, the NAS may be integral to a central server. Additionally, a RADIUS-enabled service may track users logging in or off and may also track what they have been doing. In some configurations this method of tracking may be used to charge access time for a particular service.

The RADIUS server is not limited to the authorization of usernames and passwords; it is also capable of assigning *Internet Protocol* (IP) addresses and a range of other configuration parameters, such as *Domain Name System* (DNS) addresses, *subnet masks* and so on. In particular a RADIUS server may run alongside the *Dynamic Host Configuration Protocol* (DHCP) which is used to assign users' unique IP addresses and, prior to the assignment of an IP address, the RADIUS server can be used to employ additional verification procedures. In doing so, the RADIUS protocol can request that the device must reveal its *Media Access Control* (MAC) address, which is a unique identifier assigned to all types of network capable equipment, such as a cellular phone or a computer. Once a user has been verified with a username and password, further verification can be made by crosschecking the device's MAC address. In essence, if it is not on the list of authorized devices, then the user will not be allowed to continue to use the service; however, this does bring us on to our next topic. How would an authorized user gain access to a username and password? Perhaps, a user may have overheard or read the username and password or more likely may have used a *wireless sniffer* or similar equipment to eavesdrop on the data that initially establishes a connection between a client and server. In the opening dialogue between a client and server, a hacker can intercept configuration parameters and commands, where this information can be sufficient for the hacker to *hijack* the session. Furthermore, the hacker may be capable of issuing their own commands to elude the host of unauthorized access; in turn, the hacker can fool the host into gaining access to the host's services.

WarXing: War-Walking, War-Driving and War-Storming

The processes involved in identifying vulnerable wireless networks are known as *War-Walking*, *War-Driving* and *War-Storming* (or *Flying*); these references vary from publication to publication but, in essence, they all imply the same thing. The collective term to encompass these references is *WarXing*. It still remains unfathomable as to why anyone would want to undertake such a time-consuming and labor intensive activity, despite the endless legalities and ethical issues associated with it. Perhaps this is a little unfair, as there are a *few* who are dedicated to letting people know that vulnerable wireless networks exist, and as administrators and technologists, we still need to address these outstanding issues. Nevertheless, you can easily derive from these references that they refer to a mode of transportation: walking, driving and flying. Indeed it seems that these hackers communicate in a lesser-known symbol-based language referred to as *War-Chalking*, as we illustrate in Figure 4.3. Quite simple in nature, it is derived from *hoboism* where *hobos* are homeless, but working travelers in the United States that move from city to city by freight-hopping, that is, hitching a free ride on a train. In each new area, hobos identify places within the city that are safe to occupy or, likewise, avoid areas that are dangerous through the use of chalk or coal drawn symbols. Hackers, on the other hand (or in hoboism sub-culture, *tramps* vis-à-vis itinerants who don't work but scavenge to survive),

Figure 4.3 *The series of war-chalking symbols, which are derived from hoboism sub-culture.*



utilize war-chalking as a means of identification of an available wireless network, that is, *open*, *closed* or *Wired Equivalent Privacy* (WEP) nodes (more about WEP later on in this chapter). It may be no surprise to read that many war-chalkers have dedicated resources available through the Internet; a Google.com search ("warchalking") will undoubtedly uncover many sites. Additionally, some websites offer wireless sniffing software and hardware in an attempt to make the whole hacking process that much simpler!

The premise of war-chalking is the identification of an available node and, as such, Figure 4.4 illustrates what a war-chalker would identify. In the illustration an open node that has a *Service Set Identifier* (SSID) of *Colonel* with an available bandwidth of 2Mbps has been identified. The open node reference refers to the generic availability of a wireless service; it may be the case that an administrator or home user hasn't set their service up correctly or perhaps a service provider has offered the service as free to all. Incidentally, in an attempt to overcome the proliferation of war-chalking, the *WiFi Alliance* (www.wifialliance.org) initiated a scheme to populate areas with *WiFi Zones* (www.wi-fizone.org); areas which are known open nodes that offer a free

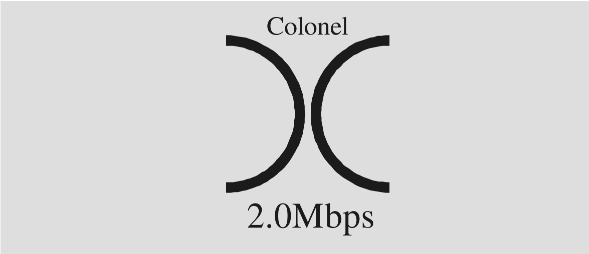


Figure 4.4 *In this example, the war-chalker has identified an open node whose SSID is Colonel where it has an available bandwidth of 2Mbps.*

Internet service. Working alongside many service providers, the website details the available open nodes in your state, country and city.

BlueJacking/BlueSnarfing

The unauthorized access to confidential information is not limited to WiFi. Bluetooth wireless technology has suffered some bad press and in particular has been associated with two new buzz words: *BlueJacking* and *BlueSnarfing* which have emerged to specifically identify the type of security attack (or weakness). Indeed, two new words for two very different problems: BlueJacking is the ability to send unwanted messages to a Bluetooth-enabled device, such as unsolicited advertising or, more significantly, the pushing of viruses and Trojans; BlueSnarfing, is the theft of private data from your Bluetooth-enabled device. BlueSnarfers will discover unprotected devices to steal data, such as calendar, contact lists and other confidential information. This type of theft is naturally deemed illegal in many countries. You may not be surprised to read that, like war-chalking, BlueSnarfing and BlueJacking have their own resources available on the Internet – some websites describe how to undertake such illegal activities. We can only assume that these kind-hearted individuals merely have the consumers' interest at heart, as they evidently wish to highlight specific weakness in the enabling of appropriate security features within a Bluetooth product.

In Chapter 11, *Bluetooth: A Cable Replacement Technology*, we discuss in more detail the security procedures that should be enabled to ensure a safer environment for Bluetooth-enabled products. Nevertheless, through lack of experience and poor education, users are inevitably not enabling the appropriate features of their products and, as such, are vulnerable to attack. Manufacturers ultimately have a responsibility to produce sufficient intelligible material informing the new user of how to configure the product securely; similarly companies that provide employees with wireless-enabled products should also educate and inform.

Encryption Principles

With reference to our initial analogy regarding security patrols and unauthorized access to offices and buildings, we can now turn our attention to *keys* and accessing private areas and/or information, as well as ensuring the integrity of our home. You may also recall that we discussed the possibility that hackers were eavesdropping on a dialogue between a client (cellular phone) and a server (wireless access point). It is during this initial phase that the username, password and other configuration parameters are exchanged to complete a connection (or session). In this section we discuss the technologies behind data *integrity* and *encryption*. Data integrity is the process whereby information that is exchanged between two devices remains unchanged as it moves across the air interface. Encryption, on the other hand, is the ability to turn a document, for example, into *ciphertext*; that is, data which is unreadable by unauthorized individuals. In essence, ciphertext can only be read by someone who is authorized to read it. When a connection is established between a client and a server, such as a user attempting to log on to an Internet service, each party will share a *common key* or *password*. When an attempt is made to establish a session with the server, the server will request that communication be encrypted, thereby ensuring that any data being exchanged between the two parties will remain private to unwanted eavesdroppers. The following sections discuss how this is achieved.

Wired Equivalent Privacy (WEP)

In addressing issues identified by war-chalkers and other various forms of eavesdropping, WEP emerged as a solution to help protect data over the air interface. As part of the *Institute of Electrical and Electronic Engineers* (IEEE) 802.11 standard, it employs two strategies to ensure confidentially and data integrity. In the former instance, cryptography (in particular, *stream cipher RC4*) is used to encrypt data over the air interface whilst data integrity is assured by using *Cyclic Redundancy Check* (CRC-32), a reliable checksum algorithm.

A checksum is used to ensure that data transmitted over the air interface is received correctly by the receiving device. The checksum is calculated using a probabilistically (or *hashing*) method, in other words, an algorithm is used to predict the data sequence in a packet. The receiving device will verify the integrity of the data packet and ensure that there have been no changes; checksum algorithms within a

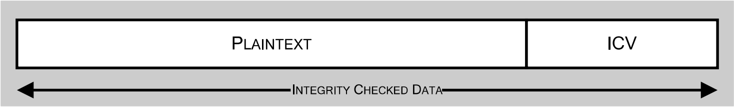


Figure 4.5 *The plaintext and appended checksum completes the data packet ready to be encrypted.*

wireless system can also be used to detect common errors, such as noise. Moreover, any changes detected within a packet may be due to hacking, where someone may have altered the contents in an attempt to hijack the session. Needless to say, if there are any changes detected within the data packet, then the receiving device may inform the source that it should send the packet again, although this doesn't apply to all wireless systems. For example, a wireless system delivering audio/video specific data remains time critical and, as such, is unable to afford the time to wait for a packet to be resent – users typically experience dropout with an audio or video signal. Prior to encryption, the calculated checksum, also known as an *Integrity Check Value* (ICV), is appended to the end of the plaintext data, as illustrated in Figure 4.5.

Having prepared the plaintext for integrity and appending the ICV value, encryption can now take place. The stream cipher RC4 (*Rivest Cipher*, named after the designer Ronald Linn Rivest of RSA Security in 1987) is a popular algorithm that is used to help protect data for fixed and wireless networks, as well as other various protocols. The premise of the algorithm is the ability to produce a pseudo-random stream of bits, also known as a *keystream*. A 64-bit secret WEP key is created through combining a 24-bit *Initialization Vector* (IV) with a 40-bit WEP key; the resulting combination produces an RC4 key. The RC4 key is then entered into a *Pseudo-Random Number Generator* (PRNG) resulting in our keystream. Finally, the keystream is *exclusively OR*'d (XOR) with the plaintext and ICV, in turn, producing our ciphertext. In Figure 4.6 we illustrate the processes involved in creating our encrypted packet and

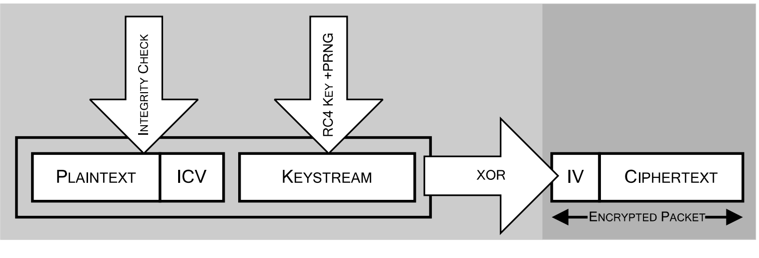


Figure 4.6 *The plaintext and ICV are exclusively OR'd with the generated keystream to produce our ciphertext. The IV value is prefixed to the cipher text unencrypted.*

you should also note that the IV value, which remains unencrypted, is prefixed to the ciphertext prior to transmission.

Naturally, the process for decrypting the data at the receiving end is reversed; remember both devices will share the common key. In a similar vein, the householder will have a key to unlock the doors and windows and, more importantly, s/he will have a key to access valuables within a safe. The RC4 key residing on the receiving device will take the IV value that was transmitted over the air and both values will be used to reproduce the keystream. Before undertaking the integrity check to ensure that there is no corrupted or tampered data, the keystream and ciphertext is finally XOR'd.

Vulnerabilities in WEP

All is not what it seems with WEP and its associated parameters used to encrypt data, as it is inherently flawed and a number of sensationalized press releases have documented its shortcomings. We will discuss in more detail the problems associated with WEP in the following section. The introduction of WEP and its bias towards the RC4 algorithm has resulted in the attacks we have experienced on WiFi equipment. Interestingly, there are several pieces of software available to download that will set about to break the encryption process employed by WEP. WEP notoriously suffered from *key recovery attacks*, where hackers made assumptions about the WEP key value based upon the value given in the IV (the unencrypted value prefixed to the ciphertext). Hacking isn't necessarily exclusive to greasy skinned geeks alone in their bedrooms accompanied with several boxes of tissues; organizations are created specifically to challenge the security ethics of a particular encryption scheme; companies such as RSA Security. It was this company, along with other academics/researchers, that highlighted the ineffective strategy within the RC4 algorithm, namely the initial selection of the IV value. Such support and constructive use of time can only ensure the future success of the technology and will ultimately help us to stay one step ahead of our critics and the hackers.

WiFi Protected Access

WiFi Protected Access (WPA and WPA2) soon emerged after several significant weaknesses were identified with WEP. WPA became ratified by the IEEE in 2004 and WPA2 is the certified 802.11i specification; there are an increasing number of products that have started to emerge onto the market that claim 802.11i certification (WPA2). Incidentally, WPA initially emerged to alleviate the immediate problems identified with WEP; in particular, business users were concerned regarding compromising data integrity and encryption. Initially, much of the WPA solution adhered to the imminent 802.11i specification, but it wasn't until WPA2 that we saw the adoption of the full specification. What we witness now are differences that render some wireless solutions incompatible, although to a greater extent WPA2 is backward compatible with WPA, but time will surely heal these inconsistencies. In Chapter 13, *WiFi: Enabling True Ubiquitous Connectivity*, we discuss the various specifications that are associated with the 802.11 standard; each specification has been assigned its own unique letter and the collective 802.11 spectrum has been typically coined within the industry as *Alphabet Soup*.

WPA now supersedes WEP; its critics (presumably the same academics and researchers that identified weaknesses in WEP) have assured us that WPA addresses WEP's shortcomings. Indeed, with several new key enhancements, namely the *Temporal Key Integrity Protocol* (TKIP), the *802.1X User Authentication* and *Extensible Authentication Protocol* (EAP) we now afford consumers greater encryption and authentication schemes. It is evident that WiFi has seen an unprecedented growth with businesses and users; both communities have believed and invested in the technology and, as such, it would be a shame and, moreover, there would be a public backlash, if their initial investment in the technology needed to be abandoned for a more secure solution. Fortunately, with such foresight implementing WPA2 into the home or office is a matter of upgrading to the latest software revision; albeit an inconvenience, it still breathes life into a technology that has already commanded a strong market share as well as satisfying its dedicated consumers.

WPA2 addresses two specific use cases: the *Enterprise* and the *home* or *Small Office/Home Office* (SOHO), also respectively known as *WPA2-Enterprise* and *WPA2-Personal*. Additional use cases are also provided for WiFi access in public places, such as *Wireless Internet Service Providers* (WISPs) and WiFi in a mixed mode environment, that is, operating a combination of WPA- and WEP-enabled devices. Nevertheless, the following discussion covers much of the crossover between these various scenarios. In the enterprise context, enhanced *Wireless Local Area Network* (WLAN) authentication is achieved through a combination of 802.1X and EAP. In conjunction with a RADIUS server, 802.1X and EAP provide effective access control and management, essentially verifying the credentials of any potential user. You may recall from our earlier discussion that access control provides a means of authentication and authorization over a LAN. In our personal context the configuration will naturally exclude the ability to use a RADIUS server; instead a *Pre-shared Key* (PSK) is used to verify authorization. The PSK can be likened to a password (this can be obtained from a user at the application level) which, in turn, becomes the *master key* used within the WPA2 implementation. If keys on both devices match, then the user is authorized to access any service. In both contexts the master key is primarily used to instigate the TKIP process.

WPA2 key management

As a result, WPA2 relies on effective key management where a number of keys are used in combination to ensure data encryption and integrity. In this discussion we will

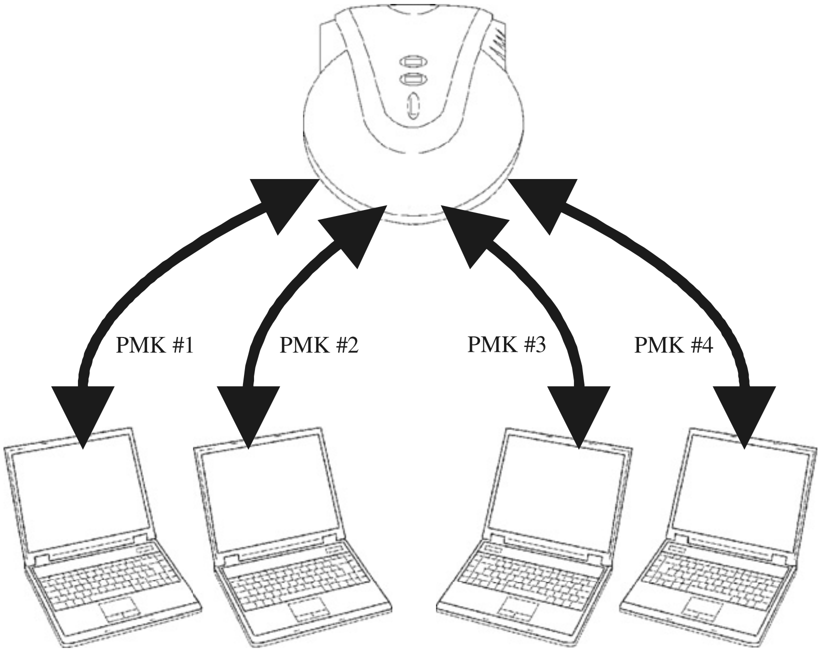


Figure 4.7
In a unicast arrangement a pairwise master key is uniquely generated for each device wishing to communicate with an access point. For each instance of device connected, a further set of temporal keys are also generated.

illustrate the number of keys that are used and we will later discuss how these keys together provide us with effective encryption and integrity. First, at the user level, as we have already mentioned, a master key is initially used to derive other keys in the WPA2 implementation. Alternatively, in some systems, a master key may be obtained from an embedded device, such as an access point. This would also be used to generate other keys within the system. The WPA2 implementation acknowledges different modes of communication; for example, if an access point is communicating with a single device, then this is referred to as *unicast* data transfer, whereas an access point communicating with many devices simultaneously is referred to as *multicast* data transfer. With these definitions in mind, keys are generated accordingly. In a unicast session, a *pairwise key* is generated to ensure one-to-one data integrity between the two devices; namely an access point with a notebook computer, as illustrated in Figure 4.7. In a multicast session, a *group key* is generated to ensure one-to-many data integrity between one or more devices, as illustrated in Figure 4.8. In each context additional master keys are further generated. In the former context, a *Pairwise Masker Key* (PMK) is created, where a group of four keys are derived from the PMK; these will ultimately be used for encryption and integrity. In a group context, a *Group Master Key* (GMK) is generated again, in turn, generating additional keys to ultimately protect broadcast communication. In both contexts, the additional keys generated are referred to as *temporal keys*, as each time the device connects to the access point new keys are generated.

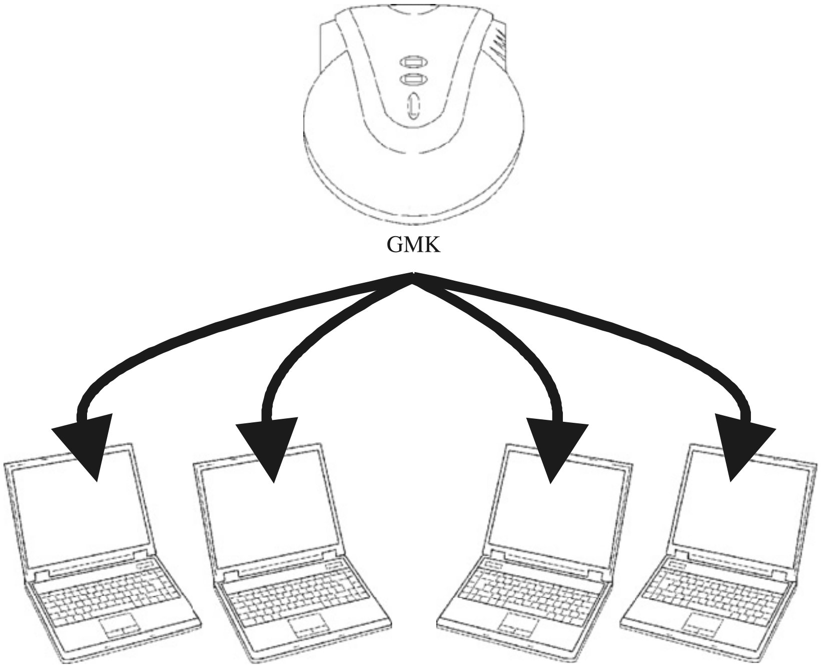


Figure 4.8
In a multicast arrangement a group master key is generated for all devices that wish to communicate with the access point. For each instance of device connected, a further set of temporal keys are also generated.

It is the constant renewing of keys and their division into unicast and multicast sessions, in addition to the creating of the temporal keys, that distinguish WEP and WPA2 implementations; WEP used a single key for unicast data encryption and invariably used a separate key for multicast. In turn, WPA2 ensures reliability in encryption and integrity; this ability is one of the advancements most noted within WPA2.

The PMK further produces four keys that are collectively referred to as the *Pairwise Transient Keys* (PTKs) where each key produced is 128-bits in length, as illustrated in Figure 4.9. The data keys are clearly used to secure unicast data transfer, as well as ensuring data validation, that is, checking that a packet hasn't been modified during broadcast. We have already mentioned the fact that these temporal keys are continually changing each time our notebook connects to the access point. To ensure this variability and, indeed, randomness, a value called a *nonce* is used during the calculation process, in addition to combining the *Media Access Control* (MAC) address of the access point; both devices know how to generate identical PMKs, as well as having already agreed particulars regarding the nonce on each device. This initial set-up and understanding is defined during session establishment or a *preauthentication* stage; such preliminary information exchanged during this phase includes the PMK. The *Extensible Authentication Protocol over LAN* (EAPOL) is used to ensure that information initially exchanged between two devices remains secure, in turn, protecting the initial credentials supplied by the client.

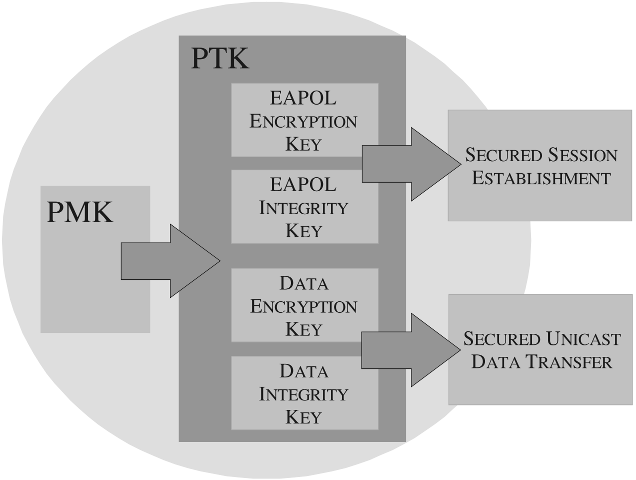


Figure 4.9 *This illustration provides a procedural flow of events that occur once a PMK has been created. From the PMK a further four keys are produced, which are collectively referred to as the PTK.*

In essence, what actually occurs after this initial preauthentication stage is a four-way handshake between the *authenticator* (our access point) and the *supplicant* (our notebook), as we illustrate in Figure 4.10. In the initial step the authenticator sends the supplicant its message containing the authenticator's nonce or *A-Nonce* (aptly the *A* refers to *Authenticator*). This, in turn, enables the supplicant to calculate its temporal keys based on the PMK value it has already received, as we discussed earlier. Interestingly, you may observe in the message sequence chart (Figure 4.10) that the data remains unencrypted. Essentially, any would-be hacker tampering with this message will result in the exchange failing. In our second stage, the supplicant submits to the authenticator its version of the nonce referred to as the *S-Nonce* (similarly, the *S* refers to *Supplicant*); again this exchange remains unencrypted, but you will notice that this time the supplicant has provided a *Message Integrity Code* (MIC or *Michael*). You may recall that WEP used an ICV that was appended to our plaintext frame (see Figure 4.6) and despite it being encrypted, hackers could not only retrieve this value by deciphering the payload, but could undertake replay attacks where data could be repeated or delayed deliberately. The MIC 8-byte value and the ICV are appended to the plaintext payload where they will be encrypted, as we illustrate in Figure 4.11. If there is no match between the PMK on both devices, then the handshake at this stage will fail.

In our third stage both devices are now ready to commence encryption where the authenticator and supplicant will have to synchronize future data transfer exchanges with each other or the handshake will subsequently fail. In this message sequence the authenticator submits to the supplicant the initial sequence reference that will instigate the encryption process. Again, from the illustration you will glean that the message remains unencrypted. In our final stage (four) which completes the four-way handshake,

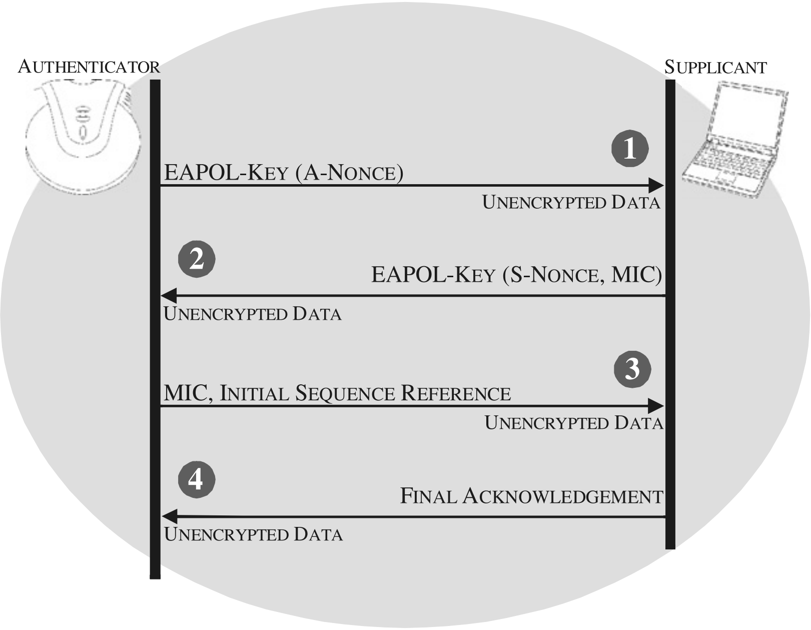


Figure 4.10 *After an initial preauthentication stage a four-way handshake between the authenticator and supplicant ensues.*

the supplicant offers the authenticator its acknowledgement of the final stage where it will now use the new keys. Both devices are now ready to encrypt future exchanges.

In our group context, only two messages are exchanged to create a secure connection. The whole process for broadcast communication is much simpler than the pairwise arrangement. In Figure 4.12 we illustrate the keys produced that are required to ensure a secured multicast data transfer. If you refer back to Figure 4.9 whilst comparing Figure 4.12 you will notice that the GMK does not use EAPOL in its set of transient keys; however, encryption and integrity keys are generated.

Initially, a 256-bit GMK is generated from a pseudo-random cryptographic number where two further temporal keys are created, collectively named the *Group Transient Keys* (GTK); the first for data encryption (128-bits) and the second for data

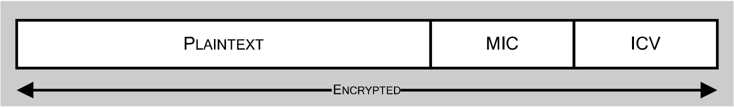


Figure 4.11 *The MIC and ICV are appended to the plaintext payload ready for encryption.*

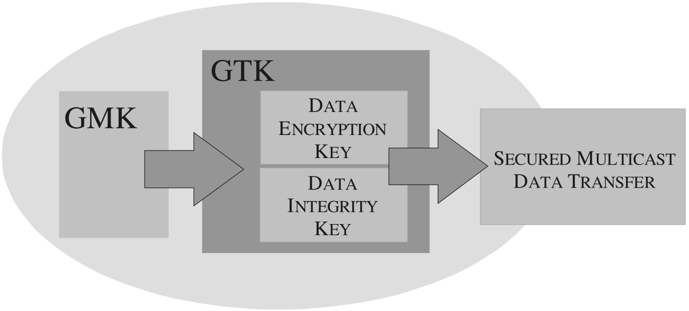


Figure 4.12 *This illustration provides a procedural flow of events that occur once a GMK has been created. From the GMK a further two keys are produced, which are collectively referred to as the GTK.*

integrity (also 128-bits). In a parallel with the PTK, the GTK is created by combining a nonce and MAC address of the authenticator. The GTK is distributed to the group of connected devices primarily to ensure privacy between all parties.

Bluetooth authentication, pairing and encryption

The premise of a good Bluetooth relationship is trust; that is, two or more devices in the potential relationship already know each other. In this first instance, if the devices wish to become more familiar with each other they enter a stage of *bonding*, which is the user's intent to fulfill the relationship. A fulfillment or, if you like, a commitment, to the relationship can be achieved with the exchange of Bluetooth *passkeys* (or passwords, very similar to our previous discussion). Incidentally, you may witness several terms being used within the Bluetooth specification, such as password, passkey and *Personal Identification Number* (PIN); these are all used synonymously, but the reference used invariably refers to different levels within the Bluetooth implementation (user level, baseband and so on) and the manifestation of its behavior at that level. We discuss the Bluetooth protocol stack in much more detail in Chapter 11, *Bluetooth: A Cable Replacement Technology*.

Authentication and pairing

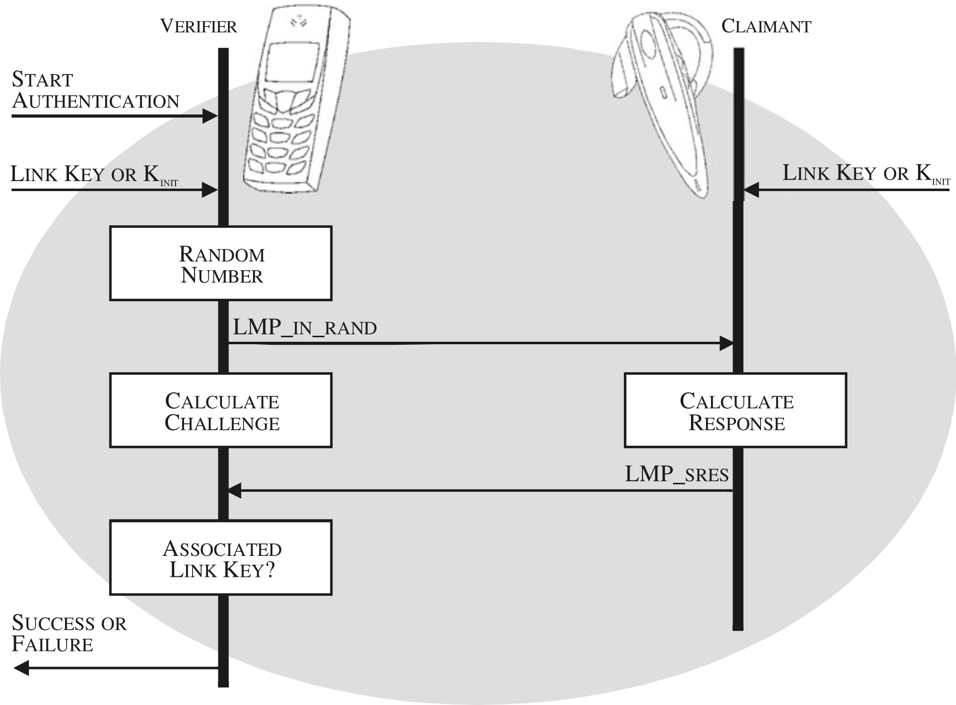
The authentication process commences when two or more devices wish to make a connection and the premise of which is based on a *challenge-response* scheme. The process establishes whether or not any of the devices have had a previous relationship, which is determined by the presence of an existing *link key*. If a key already exists then the connection can be established. However, if no link key exists, then the pairing process is initiated (we'll discuss this in a moment). The process of providing a passkey, is again, very similar to the provision of supplying a password with our WPA2 implementation. In a similar vein, the incestuous reproduction and variation of the passkey, in turn, provides numerous offspring-like keys that are used within the authentication and encryption process. This is analogous to the various PMKs and GMKs further reproducing their respective PTKs and GTKs and subsequent temporal keys. More specifically, in the Bluetooth implementation, a passkey is required as the two (or more) devices do not share a *common* link key, as we have already discussed. In this particular instance, a passkey is obtained, typically from the application level, and an *initialization key* (K_{Init}) is created in combination with a random number and the Bluetooth device's address (BD_ADDR), akin to our MAC address.

The Bluetooth specification outlines various *Protocol Data Units* (PDUs), which pertain to the behavior of a particular layer within the protocol stack. It also prescribes layer interaction and the exchange of data between such layers; additionally, the PDUs govern peer-to-peer interaction. The use of PDUs in the Bluetooth implementation bodes well for successful interoperation (more about this later) between wireless devices. In fact, the PDUs we introduce for this discussion, refer to a layer within the Bluetooth protocol stack known as the *Link Manager Protocol* (LMP), which has a number of responsibilities to perform for authentication and connection set-up. We discuss the role a layer has within a protocol stack in greater depth later on in this chapter.

In Figure 4.13 we illustrate the sequence of events that occur when the authentication attempts to establish if the two devices have or had a previous relationship. The LMP_in_rand PDU initiates the process where the LMP_sres PDU informs the verifier of its response. If the keys do not match or the devices do not share a common key, then the claimant shall respond with LMP_not_accepted informing the verifier that the key is missing. The K_{Init} is the key that is used in the initial generation of the link key within the pairing process, as both parties have only just been introduced and there isn't any history between them. It is also the K_{Init} responsibility to protect the initial exchange of parameter information when the devices are engaging in the pairing process; similar to the EAPOL within our WPA2 implementation – you may inevitably witness some duality in this discussion. You can only be reassured that these methods, albeit duplicated in various technologies, actually do the job well. As we illustrated with WEP it inherently had weaknesses in its ability to protect the data; nonetheless, the set-up and initial exchange of parameters for WEP and WPA2 to a greater extent doesn't differ from any other wireless implementation. In the Bluetooth implementation we acquire passwords and so on which inherently become primary players within the process of protecting (encrypting) data.

In Figure 4.14 we illustrate the events that lead up to the generation of a common link key as the two devices do not have any previous history. The link key is

Figure 4.13
At the start of the authentication procedure, the verifier needs to determine if there is any previous history with the claimant. If the verifier determines that there is a common link key, then the connection can be established.

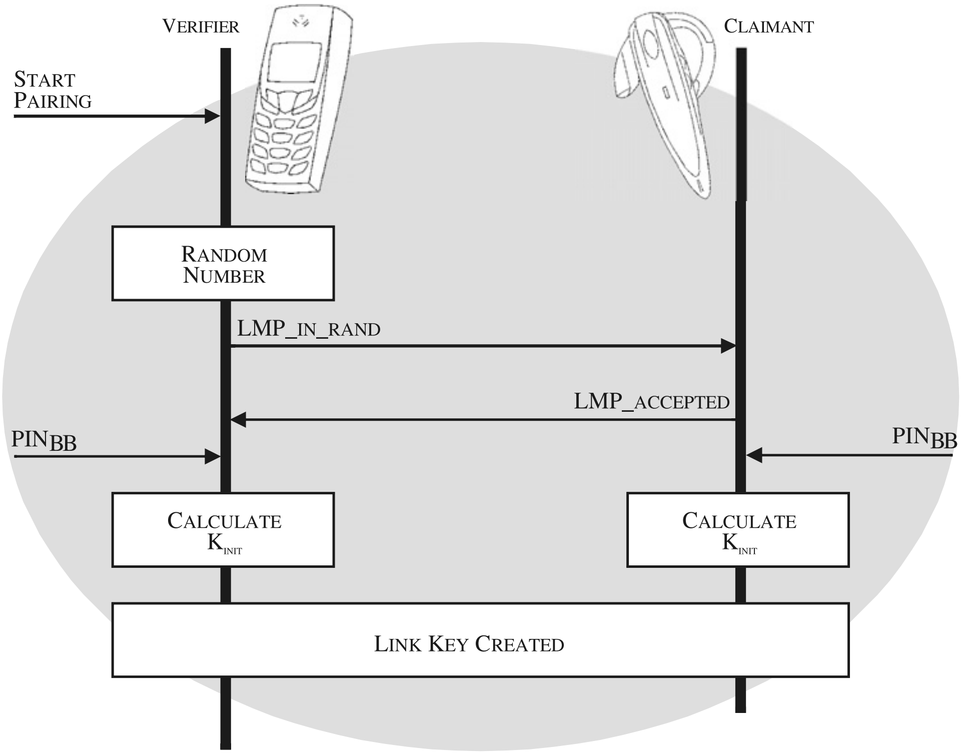


generated as a result of obtaining a passkey, as we have already discussed. You may notice from the illustration that the PIN used is at the baseband (BB) level and this is shown as $\texttt{PIN}_{BB}$ in the illustration.

Bluetooth key management

Like WPA2, Bluetooth also relies on effective key management where again numerous keys are used in combination to ensure data encryption and integrity. We have already introduced a few significant keys that are used during the authentication and pairing procedures. In this section we shall introduce the remaining set of keys that are also used within the encryption procedure. The link key, which is made up of a 128-bit random number, was introduced as a key whose primary role was to determine if two or more devices had a previous relationship and, as such, if no relationship existed a key would be generated. The link key also plays a significant role within the encryption process and, in fact, there are four types of link keys available, as shown in Table 4.1 (the unit key has now been deprecated as there were some security concerns regarding its usage within the Bluetooth implementation; this is something we

Figure 4.14 *At the start of the pairing procedure, a common link key has to be created between the verifier and the claimant. The link key is generated in part by obtaining a passkey.*



will touch upon in a moment). Additionally, there is an encryption key (K_C), which is derived from the *current* link key and is used whenever the encryption procedure is requested.

The combination key, as the name suggests, is generated as a combination of two Bluetooth devices, for example, device *A* and device *B*. And, for each new combination of device, then a new key is created. The unit key is interchangeably used with the combination key, but what distinguishes them both is the procedure used to initially create them. The unit key is generated when a Bluetooth device is installed and it is the type of application, subject to memory and storage constraints, that prescribes what key should be used (combination or unit). Since the unit key is generated only once at installation and, as such, remains fairly static throughout the lifetime of the product, this has led to its being considered unconfident in nature as a key for encryption. Instead, the combination key should be used for a more secure working environment and, evidently, more storage would be made available to these keys as they are continually generated when introduced to new devices.

Table 4.1 *The number of link keys used within the Bluetooth implementation to accommodate various application types. An encryption key is used, which is derived from the current link key*

	Key	Symbol
1	Combination Key	K_{AB}
2	Unit Key	K_{A}
3	Temporary Key	K_{Master}
4	Initialization Key	K_{Init}
	Encryption Key	K_{C}

Encryption

We introduced the initialization key in our earlier discussion, as a key that takes the role of link key during the authentication process when no other key is present; the initialization key is only used during this procedure. In contrast, the master key is used for the duration of the current connection; it may replace the original link key, since a *master* device may need to simultaneously communicate with many slaves. The initialization key is used to protect the initial exchange of parameters between Bluetooth devices, as ultimately the verifier and claimant will need to share the link keys in order to successfully authenticate and to undertake encryption. As we have already discussed, the use of encryption is optional, but if selected the E_0 algorithm is used. The E_0 algorithm is a stream cipher where individual characters in a plaintext payload are encrypted. In short, the algorithm combines (using XOR) a sequence of pseudorandom numbers with the plaintext data. It may also come as no surprise for you to read, but this algorithm has been put to the test and academics and researchers have found that the mechanism can be broken. However, it does take approximately 2^{28} iterations to successfully retrieve the key (Lu, Meier, and Vaudenay, 2005). You should consider that these tests are conducted in a laboratory-like environment where time can be afforded to study these algorithms in greater detail. Naturally, Bluetooth, by its very nature, is a portable technology, dissimilar to WiFi where access points and its users are somewhat more stationary. In other words, it may prove to be difficult to keep a Bluetooth consumer in one place long enough for someone to achieve 2^{28} calculations. In addition to this, and probably most importantly, any potential hacker would have to contend with the re-synchronization frequency which will inevitably discourage any successful attack.

The E_0 algorithm comprises three functional facets, as we illustrate in Figure 4.15. The *payload key generator* produces the payload key, which is derived from a combination

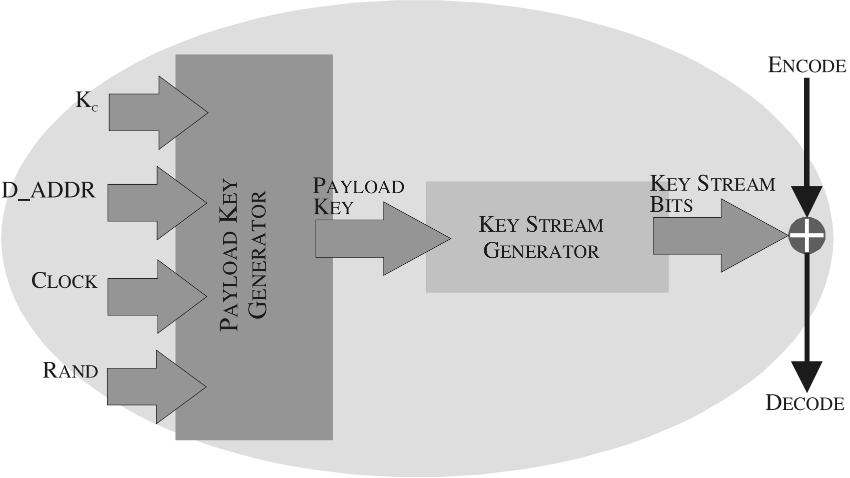


Figure 4.15 *The three facets of the E_0 algorithm comprise the payload key generator, the key stream generator and the encoding/decoding mechanism.*

of the encryption key (K_C), the BD_ADDR, the Bluetooth clock of the master device and a pseudo-random number. The second facet of the algorithm is the *key stream generator* that uses the payload key to produce the key stream bits. And finally, the third facet involves the key stream bits being encoded/decoded with the plaintext/ciphertext (that is, XOR'd).

The use of encryption, when a connection has been successfully established, is optional, as we have already highlighted. Nevertheless, if it is required, the master of the *piconet* will submit a temporary key ($K_{\mathtt{Master}}$, see Table 4.1) to one or more *slaves* informing them that this is the current link key prior to the encryption procedure. The `LMP_encryption_mode_req` PDU is used between the master and slave, as to determine if encryption is required (the mode is set to one to enable encryption). In Figure 4.16 we illustrate the sequence of events that occur during the encryption mode procedure. The slave responds with an `LMP_accepted` PDU, in turn, informing the master device that it is happy to proceed. The `LMP_encryption_key_size` PDU is used between the master and slave to agree a suitable key size for encryption. Both devices already have an idea of what key size is suitable as defined by the smallest agreeable key size ($L_{\mathtt{min}}$), but if both devices can increase this size, then a more secure environment can be established. The master device will suggest ($L_{\mathtt{sug}}$) to the slave several key sizes until such time both devices can agree. Similarly, the slave will also recommend alternative sizes it is happy to support. Once both devices have agreed a mutual key size, then the key size will be used to encrypt the connection. The slave will acknowledge that it is happy with the suggested key size with the `LMP_accepted` PDU.

In the final sequence, before encryption is started, the master will select a random number (`EN_RAND`) and the encryption key is then calculated. The `LMP_start_encryption_req` PDU is sent to the slave with the `EN_RAND`

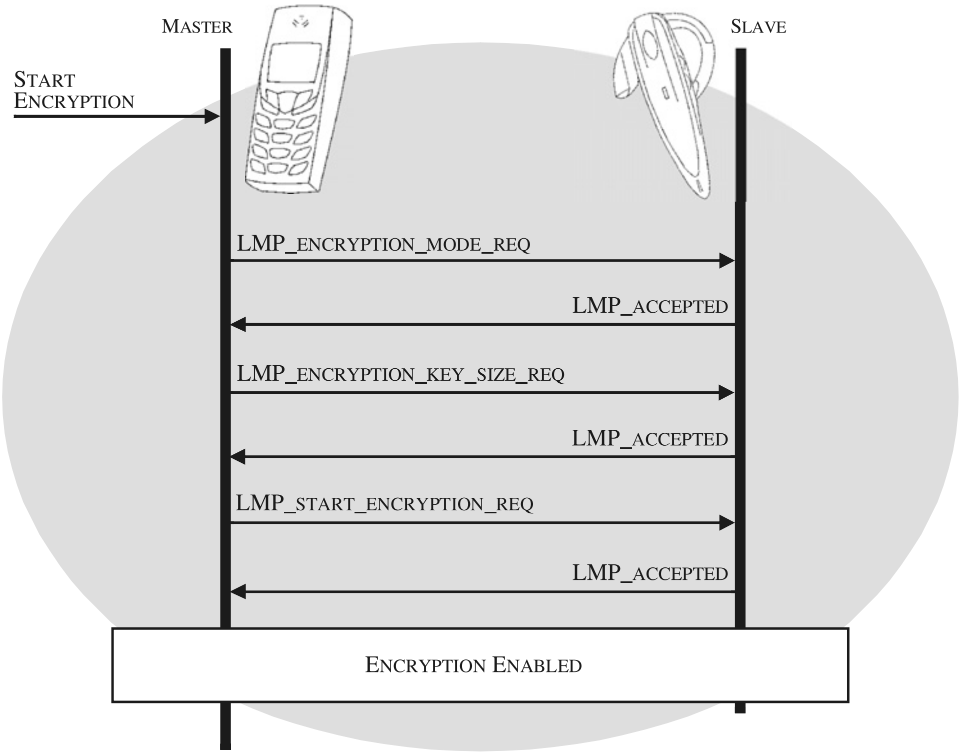


Figure 4.16 *The encryption procedure may be started once authentication and pairing have been completed. This illustration shows how the sequence of events occur for a point-to-point connection.*

attached where the slave can also calculate its encryption key. Once the slave has calculated its key and is ready to commence encryption it acknowledges that it is ready with an `LMP_accepted` PDU.

In concluding the discussion surrounding encryption for Bluetooth, you should note in Figure 4.17 and Figure 4.18 where we illustrate the basic and enhanced data rate packet formats. In particular, we highlight the fact that the payload is encrypted whilst the access code, header information and so on are sent in plaintext.

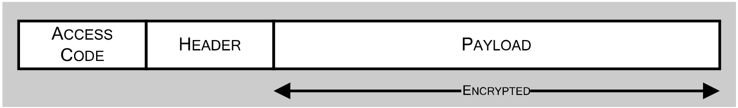


Figure 4.17 *The Access Code and Header remain unencrypted whilst the payload is encrypted prior to transmission (the standard basic data rate packet format is shown).*

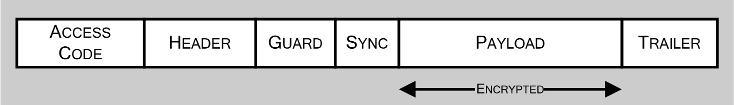


Figure 4.18 *The Access Code and Header remain unencrypted whilst the payload is encrypted during transmission (the standard enhanced data rate packet format is shown).*

But, most significantly, the E_0 algorithm is re-synchronized for every payload always ensuring variability in data integrity and security.

Despite our knowledge of the studies produced by various academics and researchers, we still haven't come across any wild speculations about possible inherent security deficiencies or prevalent compromises associated with Bluetooth authentication and encryption. The reports of Blue*Chalking* and Blue*Driving* seem to have escaped the headline news. We have merely witnessed reports of BlueJacking and the like, where users' data has been compromised due to a lack of understanding about their Bluetooth-enabled product; this is something we pick up on in the following section: *It's All About Adopting a Common Sense Approach to Wireless Security*. Empowering consumers a level of understanding that isn't conveyed as a re-education is something which we need to address when developing new wireless products and, in essence, by managing this careful balance we will begin to address common misunderstandings that are made when we rely on wireless technology.

Security features in other wireless technologies

Developing Practical Wireless Applications discusses a broad range of wireless technologies, each of which uniquely imparts its own capabilities and features enabling a rich host of applications. Unavoidably, as each new technology is introduced, so too is a set of security features that individually characterizes a capability to minimize attacks or *Denial of Service* (DoS). In each of the respective chapters that discuss a wireless technology, we take an opportunity to disclose a level of technical detail that should be sufficient for you to understand the security features of that technology. In our earlier sections we discussed two very popular technologies, Bluetooth and WiFi, as these technologies to a greater extent dominate the consumer's perception (for the time being). Running up behind these technologies we have *Near Field Communications* (NFC), ZigBee and UWB, all of which may complement or compete. Nonetheless, we have chosen to discuss these particular technologies as they both typify many of the limitations that wireless technologies continue to impose, and similarly, we need to constantly be thinking ahead or in short, perhaps adopt a common sense approach to wireless security.

It's All About Adopting a Common Sense Approach to Wireless Security

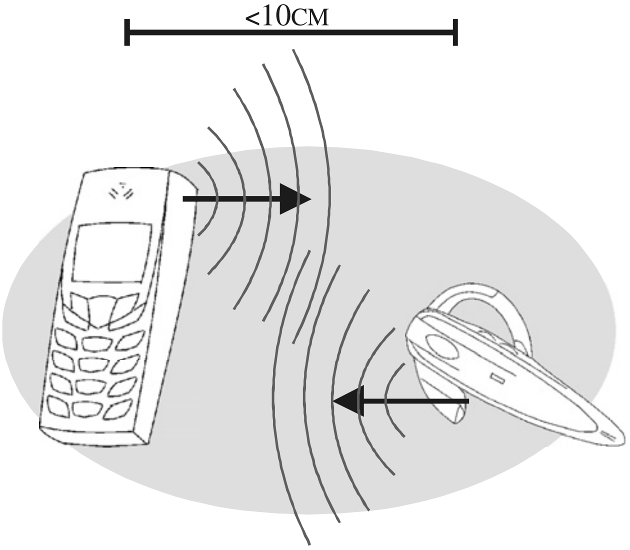
We can liken the adoption of a common sense approach to security to that of securing our house when we leave it unoccupied. In somewhat of a paradox, manufacturers and consumers need to be aware of utilizing the inherent security features of their wireless products. On one hand, we would encourage an out-of-the-box experience whilst, on the other, we have the inescapable need of the consumer digesting relevant information surrounding security configuration. In such a dichotomy we need to establish a comfortable balance between *need to know* and *want to know*. Perhaps we should consider some default settings where the consumer is pushed into configuring their device and, no doubt, we could spend an eternity deliberating what could or should be done. Nevertheless, when we leave our house we always check the windows and doors, ensuring the property is secure. Why can't we extend this notion to ensuring that the most basic of wireless security requirements are met?

Initially in this chapter we discussed the sensationalized reports of BlueJacking, WarChalking and so on. In the former example, we can alleviate such characterization by simply requesting that all Bluetooth-enabled devices require a passkey or alternatively, switching off discoverable mode (or perhaps enabling both features). Essentially, this configuration can be made as default, ensuring that the wireless device is already secure at the onset (or out of the box). In the WarChalking instance this exemplifies the weakness of the inherent security or an administrator's naivety with WEP/WPA configuration within the device and, as such, technologists have proactively ensured that safer authentication and encryption schemes are used. In a similar manner to that of the Bluetooth device, manufacturers can also define default settings, again ensuring that the device is secure – straight out of the box. No doubt we will continue to see hackers and the like persistently attempting to crack a code or two, but if we ensure that the window is locked and the door is closed, then it should become increasingly difficult at the start for a hacker to look in.

Enabling Intelligent Connectivity

In adopting a common sense approach to wireless security we clearly still assume that consumers will be au fait with wireless terminology and usage. And, in an attempt to simplify the need to be familiar with such terminology perhaps we should consider a more intelligent approach towards enabling connectivity. We discuss one such example in Chapter 14, *Near Field Communications: The Smart Choice for Enabling Connectivity*. The premise of a more simplified mechanism for connectivity is based upon the consumer's *intent* to connect. In other words, if a consumer wishes to connect his/her Bluetooth-enabled cellular phone to a Bluetooth-enabled headset, then the consumer brings together the two devices where they both transparently connect, as we illustrate in Figure 4.19. In this particular example, the authentication and configuration parameters remain oblivious to the consumer, and in utilizing NFC over Bluetooth, the parameters are exchanged seamlessly between the two devices ensuring that the right devices are connected! Similarly, a WiFi access point in an airport can be made available to the commuter. The commuter would simply approach the access point with his/her PDA or notebook notifying the access point that this device intends to connect to it. Overcoming security concerns are in effect momentarily put aside with this particular anecdote. With an intent and proximity of connection in mind, you may find yourself in a situation where you may witness an individual who has invaded your private space and is persistently moving his or her cellular phone about your person – you can only assume that you know this person very well or you don't mind that person invading your space as s/he is particularly gorgeous or, the more likely conclusion, is that the individual is attempting to access private and confidential information! Nevertheless, your wireless device has its default settings enabled and, additionally, as part of the default mode, you may request that any device wishing to connect to your product has to be authorized with a "yes" or "no" confirmation. Presumably, if this individual managed to invade your space without your knowledge, then the user interface would prompt you to make the confirmation and after a period of time will assume "no" as you haven't intervened.

Figure 4.19 *NFC has a short range of around 5 to 10cm and to enable connectivity the user must bring these devices within range.*



The use case extends beyond connecting devices. It may be used in a variety of contexts where access to secure areas is required or, as we discuss in Chapter 5, *Realizing a True Wireless Life-style Vision*, a number of scenarios are given where the character "David" can seamlessly access buildings, secure parking and his personal computer using a single smartcard. Moreover, this isn't a new technology, as we already have existing technologies enabling us to access buildings, secure areas and personal computers, but the various contexts highlight the user's intent to connect, access an area and so on. This premise lends itself well to a more intelligent ability to connect and, most predictably, to answer those skeptics among us; yes, if you lose your smartcard the user's security becomes compromised. Many technologists have speculated with the notion of enabling your cellular phone or a key fob with this intelligent connectivity but, of course, people lose their phones and their keys too. The solution to this approach is contained within our ability to terminate our *Subscriber Identity Module* (SIM) with your network provider when you lose your cellular phone and, of course, we cancel credit cards and so on when we lose our wallet. Yes, of course it's an inconvenience, but you can be assured that the smartcard and cellular phone are protected from any unauthorized use.

Coexistence and Interoperation

Coexistence and interoperation are definitions that have haunted the development community for a number of years and still do today. Coexistence is characterized by a number of wireless devices in proximity which use the same radio spectrum (for example the overcrowded 2.4GHz band) or where a wireless device simply needs to coexist with a number of other wireless-enabled devices that may not share the same radio spectrum. In an environment where one wireless device needs to coexist and doesn't do this successfully then the user will experience degradation in bandwidth and, as such, a poor quality of service, or even harsher, won't be able to connect to any wireless-enabled device at all. Interoperation is characterized by successfully connecting a device from manufacturer *A* to manufacturer *B*. For example, if manufacturer A has developed a Bluetooth-enabled cellular phone and it supports the headset profile (see Chapter 11, *Bluetooth: A Cable Replacement Technology*) it should interoperate with any Bluetooth-enabled headset. However, in this instance, manufacturer B develops the headset product. Irrespective of origin, if both devices support the Bluetooth headset profile, then both devices should support the features as defined by the Bluetooth specification. In other words, both devices should work harmoniously and interoperate successfully. What some manufacturers provide is a number of features that are enabled when you have two products provided by the same manufacturer. For example, if manufacturer A has developed both the cellular phone and headset,

Figure 4.20 *The plethora of wireless devices seemingly creates an innocuous and invisible voice and data stream which remains inaudible to the human ear and invisible to the human eye. We are constantly surrounded by various ranges of invisible spectrum which, as if by magic, enables a host of applications we have already become familiar with.*

then the cellular phone would recognize that it is provided by the same manufacturer and extends the available features above and beyond the Bluetooth specification. Nevertheless, both products do comply with guidelines as defined by the Bluetooth *Special Interest Group* (SIG) as they meet the mandatory requirements as governed by the Bluetooth specification. The additional features that are out of the scope of the Bluetooth specification will ultimately need to interoperate successfully with the recognized hardware, but the scope of this successful interoperation shall need to be addressed by the manufacturer. It is certainly true for WiFi and its associated range of products, as some manufacturers have devised their own flavor of WiFi bandwidth which is out of the scope of the IEEE 802.11 specification. In these instances these manufacturers have captured a market share that doesn't have to wait for the next revision of the specification to be released and today consumers can enjoy the benefit of greater bandwidth now. In short, many companies have offered 802.11b access points (supporting 11Mbps), but if you purchase their client then you will enjoy a bandwidth of up to 22Mbps and so on. Similarly, as the respective specifications are released (802.11g and 802.11a) so to does the bandwidth double if you become loyal advocates of the manufacturer and buy into their bespoke technology.

Taking the technology back to its core definition, that is, back to the original specification, how do manufacturers and developers overcome coexistence with the crowded arena of wireless devices that seemingly create an innocuous and invisible voice and data stream which remains inaudible to the human ear and invisible to the human eye (Figure 4.20)? In the sections that follow, we discuss the mechanisms that are available to manufacturers and developers that reduce the likelihood of interference and encourage successful communication with a myriad of wireless products.

Ignoring unwanted noise

Most of the wireless technologies and their associated bodies presented within this book have considered the problems associated with operating multiple devices in proximity. The architecture of these technologies has first and foremost been crafted to overcome or inhibit some of the problems associated with coexistence. And, indeed it's an important issue and a priority for the many governing bodies associated with these technologies, such as the Bluetooth SIG, WiFi Alliance and the ZigBee Alliance.

In a constant stream of new ideas and technologies, each purporting a range of capabilities that are superior to its nearest competitor, all technologies have to coexist in an already crowded environment. The early Bluetooth products didn't penetrate the US market successfully as there were already numerous proprietary technologies offering bespoke capabilities to a host of industries and manufacturing. With a need to create deeper market penetration and to overcome coexistence with WiFi, the Bluetooth SIG devised a mechanism to help alleviate coexistence of its Bluetooth-enabled products. *Adaptive Frequency Hopping* (AFH) is a scheme that was introduced by the SIG to reduce interference with a range of proprietary technologies that already use the 2.4GHz radio spectrum and, of course, wireless LANs. The initial set of WiFi products supported the 802.11b and 802.11g, which both use the 2.4GHz radio spectrum and, naturally, the market growth of WiFi and these initial products has been phenomenal. More specifically, the nature of the problem was due to a frequency hopping scheme, hopping at a rate of 1,600 times per second where the scheme would utilize the 79 channels available in the 2.4GHz band. The new generation of Bluetooth products uses AFH to avoid conflicts within the available channel range. In an environment where there are many 2.4GHz wireless products, there was a greater probability that a collision would occur on a particular channel and, as such, data would be lost. AFH affords Bluetooth a more intelligent approach to its frequency hopping scheme, as it adapts to the environment in which it finds itself. If there is a consistent problem with a particular channel, then AFH will exclude this channel from the scheme. Interestingly, in a heavily populated environment, it is conceivable that the number of available channels would reduce considerably; however, the specification does dictate that the minimum number of channels readily available should be around twenty. Although the scheme helps reduce the likelihood of problems associated with coexistence it is still not completely dependable. The Bluetooth SIG is not alone in resolving interference issues. The IEEE 802.19 Wireless Coexistence *Technical Advisory Group* (TAG) has been specifically formed to consider future improvements of the 802.11 technologies. The group aims to produce a report, titled "Recommended Practice for Information Technology – Telecommunications and Information Exchange between Systems – Local and Metropolitan Networks – Specific Requirements – Part 19: Methods for Assessing Coexistence of Wireless Networks" in 2008, which will offer assistance and guidance for standards that operate in the unlicensed spectrum.

Presumably, technologies like ZigBee should be included and governed by this future report, as the radio specification for the technology is produced by the IEEE in the 802.15.4 specification. Although ZigBee does make use of the unlicensed 2.4GHz band, it does utilize two others, namely the 868MHz band for Europe and the *Industrial Scientific and Medical* (ISM) 915MHz band for the Americas, where the number of available operating channels vary (more about this in Chapter 12, *ZigBee: Untethered and Unlicensed*). Like WiFi, ZigBee uses a combination of techniques to include *Clear Channel Assessment* (CCA) and is particularly appropriate for low bandwidth devices in establishing a more harmonious coexistence with other 2.4GHz-enabled products. ZigBee combines CCA with a technique called *Carrier Sense Multiple Access with Collision Avoidance* (CSMA-CA) to alleviate issues with multiple ZigBee devices. CSMA-CA reduces the likelihood of multiple ZigBee devices communicating simultaneously and uses a *jamming* mechanism to achieve effective communication. Assuming our communication pathway is clear or, at least, there is an intelligent means by which one device can to take with another, how do we ensure devices interoperate successfully?

How can we talk with each other?

The definition of *interoperable* (interoperate, interoperation, interoperability) is not restricted to successful intercommunication between products. It can also be extended to include various software applications that have to share data with each other or it can be referred to numerous business procedures within an organization. For example, one department talking to another or simply when there is a particular method of buying and selling commodities. Interoperation, in this context, refers to the ability for key business processes maintaining effective intercommunication. For the sake of this discussion, we will restrict our dialogue to include interoperability of wireless products with one another that may be supplied by multiple manufacturers. As we have already indicated, software applications can also interoperate, but here we will discuss how the nature of a wireless product, in terms of its hardware and software attributes, permits the ability to successfully communicate and to understand one another. In Figure 4.21 we introduce the *International Standards Organization*'s (ISO) *Open Systems Interconnect* (OSI) model. The model encourages developers to establish a common foundation upon which communications-based systems can successfully communicate and, most importantly, interoperate. The model was introduced circa 1984 to assist the development community in establishing consistent intercommunication between communication-based products, as there was somewhat of a disarray within the telecommunication industry.

The model achieves interoperation through a peer-to-peer topology; but before we discuss this in any detail, we should consider the actual layers in our OSI model. In the model we depict seven layers, each of which has a unique role to play. Each layer is an independent entity and, like a black box, takes in data at one end and outputs data at the other. A layer understands how it should talk to its adjacent layer(s) through an *Application Programming Interface* (API); each layer supplies its adjacent layer with the data it requires and only the data it requires. The layer receiving this information may decide to process this data further by sending its response down the model or up the model. The application layer is the layer at which the user will interact with the application, whereas the physical layer is the entity that will interact with the physical hardware (like a radio for example). You may recall from our discussion surrounding Bluetooth authentication, pairing and encryption, we introduced a

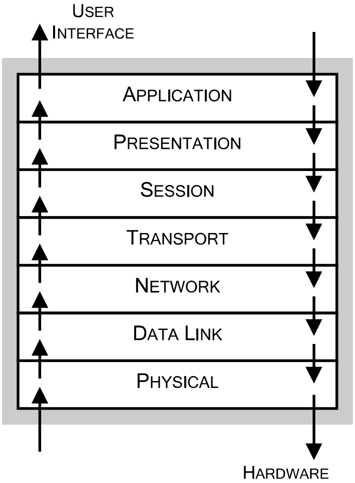


Figure 4.21 *The OSI Model forms the basis of good interoperation and is prolific in many communication-based products. The user will interact with the application layer through a user interface for example; on the other hand, the physical layer interacts directly with the connected hardware.*

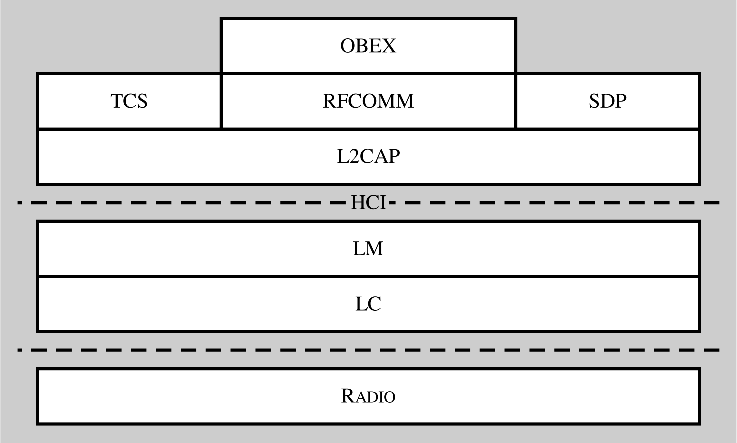


Figure 4.22 *The numerous layers that uniquely form the software building blocks of the Bluetooth protocol stack.*

number of PDUs which would be used to enable functionality within the Bluetooth-enabled device. If you have two devices, such as our master and slave, the PDU would specifically be referring to the LMP layer of the Bluetooth protocol stack, as we discussed earlier. In Figure 4.22 we illustrate, for this example, the Bluetooth protocol stack and the layers that make it up.

A layer in device *A* will communicate with the same layer in device *B*, that is, physical to physical, data link to data link and so on – this concept is referred to as peer-to-peer communication and in Figure 4.23 we illustrate the conceptual nature of peer-to-peer communication. Furthermore, in a Russian-doll fashion, when a user request is made from the user interface (the application layer), the request is moved down the stack where an action maybe performed; this may result in an over the air transmission via the physical layer to the radio. As the request reaches each layer,

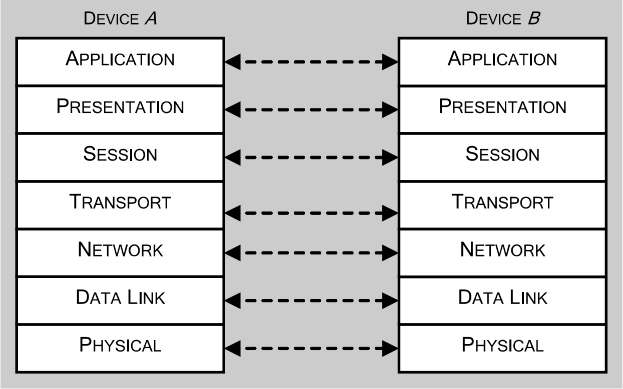


Figure 4.23 *In a peer-to-peer topology the layer of one device communicates with the respective layer of the other device and vice versa.*

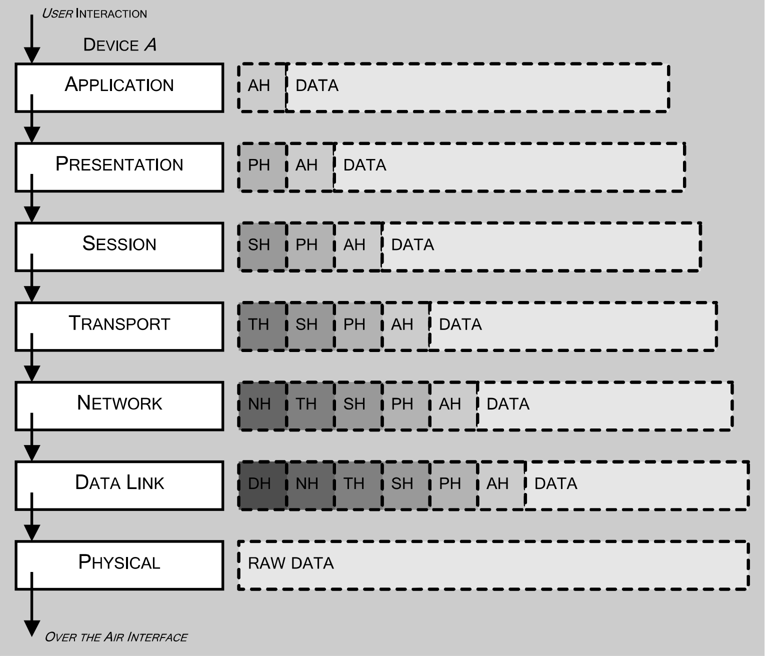


Figure 4.24 *A user will interact with the software via the user interface. The request is packaged up in a Russian-doll like fashion where each layer appends its own header information. The receiving device will disassemble its respective header to learn about what needs to be done.*

the respective layer will decide on what actions are required. It may be the case that the user wishes to learn more about device B and, as such, the request is ultimately moved down the protocol stack for the physical layer to transmit its request to device B. In Figure 4.24 we see the Russian-doll encapsulation of the request as it is assembled and moves down the stack where each layer appends its own header information.

The receiving device (B) will disassemble each header as it arrives at the respective layer. In one such example, if device A wishes to connect to device B, the user of device B will need to authorize the connection by informing the user of device B at the user interface. Device B will be promoted to authorize the connection with a “yes” or “no” response. The response will be assembled and sent down the stack where it is transmitted to device A.

The OSI model is the basis of the majority of (if not all) communication-based technologies, such as Bluetooth, WiFi, ZigBee, NFC and so on. It remains a traditional and widely accepted method of developing protocol stacks that can be transported to product to product.

Summary

- Many books have been dedicated to the security of wireless technology.
- Consumers who want "out of the box" solutions are the ones who will experience a new wireless product's security inadequacies first-hand.
- Due to wireless' innate invisibility, consumers may not realize a security breach until it's too late.
- Security is crucial to the success and future of wireless technology.
- Consumers and companies need to be confident that their data is secure.
- With recent reports of War-Driving, War-Walking, War-Flying, Phishing, BlueJacking and BlueSnarfing, can we be certain that our wireless networks and their stored data are secure?
- The architecture of wireless security can be likened to the requirement of a secure home – that is, securing its contents, its perimeter and surrounding grounds.
- Our locked doors and windows may become compromised as they can be forcibly opened, but with the availability of security alarms we can help further deter unauthorized access.
- Any individual attempting to access a secure wireless network will be challenged by the host (or server).
- Like the host of a computer network, a security officer will request identification ultimately to determine if you're an authorized user.
- The host will request that you supply a username and password to successfully enable you to gain access to the wireless network.
- Access control refers to the means by which a user can successfully gain access to a service, which is available through a LAN, WLAN or WAN.
- RADIUS is a de facto industry standard protocol, which is used to verify users of a particular service through a centralized database such as a NAS.
- Usernames and passwords are crosschecked with the database to ensure that the user is authorized.
- A NAS may include a VPN or a wireless AP, but typically, in a larger organization, the NAS may be integral to a central server.
- The RADIUS server is not limited to the authorization of usernames and passwords; it is also capable of assigning IP addresses and a range of other configuration parameters, such as DNS addresses, subnet masks and so on.
- The RADIUS protocol can request that the device must reveal its MAC address, which is a unique identifier assigned to all types of network capable equipment.

- The processes involved in identifying vulnerable wireless networks are known as War-Walking, War-Driving and War-Storming (or Flying).
- The premise of war-chalking is the identification of an available node.
- The open node reference refers to the generic availability of a wireless service.
- The unauthorized access to confidential information is not limited to WiFi. Bluetooth wireless technology has suffered some bad press.
- BlueJacking and BlueSnarfing have emerged to specifically identify the type of security attack (or weakness) against Bluetooth wireless technology.
- BlueJacking is the ability to send unwanted messages to a Bluetooth-enabled device.
- BlueSnarfing is the theft of private data from your Bluetooth-enabled device.
- Through a lack of experience and poor education, users are inevitably not enabling the appropriate features of their products.
- Manufacturers ultimately have a responsibility to produce sufficient intelligible material informing the new user of how to configure the product securely.
- Companies that provide employees with wireless-enabled products should also educate and inform.
- We should adopt a common sense approach to wireless security.
- We can liken the adoption of a common sense approach to security to that of securing our house when we leave it unoccupied.
- In adopting a common sense approach to wireless security we of course still assume that consumers would be au fait with wireless terminology and usage.
- Perhaps we should consider a more intelligent approach towards enabling connectivity.
- A more simplified mechanism for connectivity is based upon the consumer's intent to connect.
- If a consumer wishes to connect his/her Bluetooth-enabled cellular phone to a Bluetooth-enabled headset, then the consumer brings together the two devices where they both transparently connect.
- Coexistence is characterized by a number of wireless devices in proximity which uses the same radio spectrum or where a wireless device simply needs to coexist with a number of other wireless-enabled devices.
- In an environment where one wireless device needs to coexist and doesn't do this successfully then the user will experience degradation in bandwidth.
- Or even harsher, won't be able to connect to any wireless-enabled device at all.
- Interoperation is characterized by successfully connecting a device from manufacturer *A* to manufacturer *B*.

- In a constant stream of new ideas and technologies, each purporting a range of capabilities that are superior to its nearest competitor has to coexist in an already crowded environment.
- The OSI model encourages developers to establish a common foundation upon which communication-based systems can successfully communicate and, most importantly, interoperate.
- The model achieves interoperation through a peer-to-peer topology.

5

Realizing a True Wireless Life-style Vision

In this chapter we tell of an Arthur C. Clarke moment where we have, for the duration of this chapter, a unique insight into the science of how the *true wireless life-style vision* should be experienced. This is not a prediction nor the narrative of an honored scientist, but merely the vision of an author who remains passionate about wireless and who endorses a supportive experience. We continually, blindly thrust wireless technology into consumers' faces and expect them to know everything. Do we translate this into a wireless vision or deem it a myopic dysfunction of an unguided community? Let's move beyond a necessity to educate and to make assumptions about our audience, and, instead, let's infuse the expectation of an untethered experience. If you already have some familiarity with a product and manufacturers have incidentally made it wireless there shouldn't be a need to re-educate but simply to operate the product as you did before (except without the cables). In this fictitious narrative, albeit passionate, we contemplate the whole living/working life-style, that is, waking-up in the morning to going to bed at night. The expectation of this familiarity is comparative to the use of the cellular phone. Moreover, we use a phone to make and receive calls – consumers, to a greater extent, don't consider this device in anyway *wireless* (naturally the individuals in-the-know should); it ultimately performs a function and this, in turn, is our pinnacle objective; to look beyond the product as a means of configuration and set-up, and instead as a product that is switched-on and works. It's only recently that advocates of wireless technology have realized that consumers need an *out-of-the-box* experience whereby the packaging is removed and the product is ready to interoperate with any device. In essence, you only have to switch it on!

Defining Quantitative Needs for Technology

Network operators and cellular phone manufacturers have achieved this differential over an approximate twenty-year period; amusingly, a time that has witnessed a cellular phone the size of a house brick transformed into a device that sits comfortably in your jean pocket. If you purchase a new phone today, it is indeed an out-of-the-box experience, as you simply remove the packaging, insert the battery and *Subscriber Identify Module* (SIM) card. Once you switch it on there is no configuration or set-up, you just automatically become connected to the network operator's service. Admittedly, operators and manufacturers are *now* dipping into a need to increase revenue with value-added services which, in turn, encourage a more diversified life-style in supporting an on-demand ethos where you are led to believe you have to have it now. In the United Kingdom and Europe, mobile TV (that is, broadcast-like video on a cellular phone) is becoming increasingly prevalent. The initial marketing drive for this application was the ability to witness and to visually interact with the incoming caller through video (gone are the days where you can roll your eyeballs when you receive a call from your boss and you're home *sick*). The unequivocal momentum driven by operators who *know* that consumers need this service is perhaps somewhat misguided. The drive should be smooth and should ultimately encompass more than getting from A to B; an evident need to have TV on your cellular phone should be more than an argument of "well, we can." Nor is it a contest between operators: "yep, we did it first," but more importantly, a drive that is solely based upon consumers' needs and expectations. "I *do* want to see my boss on my phone, so that he really can see me ill at home," is one such statement from an honest consumer (the irony is way off the scale right now!). Seriously though, in the United Kingdom several network operators are undertaking trials of cellular technology where it envisaged that approximately 80% of the existing consumer-base (that is, those who already have a cellular phone to support such a service) would subscribe to receive a mobile TV service. The initial expectation has now morphed into a definable need from consumers who, once they've experienced the technology, now think they could benefit from receiving up-to-date information on their cellular phones. As such, it is predicted that these consumers would not want to view an entire film, but would be more inclined to receive snippets of information such as film trailers, breaking news features, soccer scores and pornographic material (yes, pornographic material!). This gathering of more relevant information enables us to move forward from an ethos of "well, we can" to the provision of a service that is quantified by a potential community that is prepared to levy a budget and benefit on such an advantageous service.

Okay, let's take an opportunity to refocus on our primary objective in this chapter which is to understand what consumers might experience in a lucid wireless vision. Using the aforementioned comparative example of a cellular phone, how can we achieve the same transparent wireless operation and create a comparable use of personal-area wireless technology? A typical day for most people is to get up; go to work; drive home; spend more time on work; watch some TV (on the big box in the corner of your room); go to bed; undertake some nocturnal activities – sleep that is! "Eeeek!," such a harsh cold reality. Anyway, let's ignore the functional aspects, but simply elaborate on the everyday facts. For this narrative we shall place in our context David and Louise; they are a semi-professional couple that have a one-year-old daughter, Daisy. The basic premise of this tale is to discover how David and Louise might interact with technology within their home, which is intrinsically wireless-enabled and connected to a wider fixed infrastructure, and how they might interact with technology away from the home – at work, for instance. Similarly, we need to avoid a sense of "I'm trying to make my wireless connection work," Patrick Stewart, *Eleventh Hour*, 2006, ITV1, United Kingdom, and the seemingly confident finger movements across a keypad where, as if by magic, the connection is established. Instead we focus here upon a second nature where the technology itself knows how it should work, something along the lines of self-awareness and self-configuration. Indeed, you may also be somewhat bemused as to why a chapter such as this exists within a technical book. Arguably, if you finish this chapter and conclude that this was a story of a young couple and their daughter who unobtrusively interacted with a number of wireless-enabled products, then the author has indeed achieved his objective: technology should remain *supportive* and *incidental*, and this story describes one case study of how this might be achieved. Think of this chapter as means of shaping your perception about wireless technology and perhaps refocusing how it should be received by others (our consumers). If you like, take it as a template or blueprint that may be used over time, allowing it to evolve into a more valuable and complete reference.

In Technology we Trust

It's 6:00am: the alarm goes off – nothing particularly wireless about this event, but indeed David and Louise wrestle in bed much to their discomfort in the realization that it's morning. In an habitual routine, David hits the snooze button to capture an extra ten minutes and, as we can all recognize, inwardly mutters "that wasn't ten minutes, surely?" when it goes off again. Dutifully, David enters the shower and Louise attends to their daughter and carries her downstairs to make the coffee. David isn't much of a morning person and takes the opportunity to shower in order to ultimately wake up. Louise, on the other hand, has instinctively performed the role of mother since she left her high-profile marketing executive position in New York two years ago and attends to her daughter, who is naturally delighted to see her. Daisy was monitored for the duration of her sleep by a device that is wireless-enabled; a product that can be purchased from any store. In David and Louise's home they have an integral audio system that supports playback from audio devices such as the HiFi, MP3 player, telephone and TV. Each room has a speaker system installed allowing them to hear music or TV in any room. Additionally, a wireless baby monitor joins the list of audio devices where David and Louise can hear the slightest movement from Daisy's bedroom.

For example, during the “watch some TV” routine they are able to listen to the integral speaker system (in Dolby surround) in their family room. Nevertheless, if the baby stirs to a decibel level that may cause concern, the wireless baby monitor notifies the integral system which, in turn, interrupts the TV viewing, pauses the programme and mutes the sound. Louise and David can now listen to the motion within Daisy’s room where presumably Louise and David can now discuss who will attend to her. Louise (naturally) attends to her daughter as David is watching the New York Yankees – he’s not going to move!

David and Louise purchased a new build property on the outskirts of New Jersey and one of the attractive features of the property they found was the integral smart home system which aimed to simplify living. The advertising avoided any bold statements of talking refrigerators and portrayed an image of simplicity and the harmonious interaction of devices within the home. It reinforced the fact that the technology did not demand any prior technical knowledge, but merely offered an intuitive system that was already pre-configured to *meet* their expectations; in other words, it was set up to enhance how they chose to live. David and Louise were asked to name their home system, and after some bewilderment, they named it Nora after Louise’s best friend. It would mean that either David or Louise could partially interact with Nora through voice commands. You are probably questioning that this notion isn’t entirely new and indeed you’d be right. However, the prevalence of such a smart home system is not as widespread as you might expect, especially since the technology is already available. The top-end property market might enjoy such systems but, as we discover, the notion of simplicity has eluded most manufacturers. We should question the simplicity afforded within the home security system installed in these rather exclusive homes. Again, maybe we are faced with the development ethos of “well, we can” and manufacturers still remain oblivious to customers’ needs and expectations. Moreover, maybe we need to understand the definitive need and enjoy reflective contemplation of technology within the home. Chapter 7, *ZenSys: An Open Standard for Wireless Home Control*, and Chapter 12, *ZigBee: Untethered and Unlicensed*, offer some insight into the technology that is being offered as a smart home solution. Let’s be honest with ourselves here; your washing machine, toaster and refrigerator don’t need to be connected to the Internet – why on earth would anybody wish to switch on a washing machine remotely? Can you imagine the fun hackers would have drumming up an increased service bill? In Chapter 1, *Making Sense of Wireless Technology*, we talked of applying a sense of proportion and reality, and undoubtedly the home is no exception. Equally as important, incorporating wireless technology into any device should ultimately obey the principle of adhering to a sense of proportion and reality. We have to face some kind of realism in new product development; put aside the prospect of bleak bank balances and affect upon stocks and shares, as making a bad decision would inevitably paint the future red anyway. It seems all too easy to put pen to paper and make incredulous statements, but there is never an easy answer to life, the universe and everything, although Deep Thought* felt differently. Deep Thought was unable to provide an answer to this all-knowing question, as the set of parameters or information he was initially supplied with was insufficient and perhaps ambiguous. We can use a similar analogy in terms of making new product development decisions, as we will always need to instigate a new project with all the appropriate information in front of us before we proceed and engage in a financial commitment. Nevertheless, as you are already aware of, there is no degree of certainty in your success; as prepared as you might think you are with the right market or technical information, the product still might not be a success. That killer application still eludes us!

Back to David and Louise: they purchased their dream home and furnished it with hand-me-down furniture donated by various relatives (it is after all their first home and David can no longer rely on Louise's second income), although Louise does work part-time occasionally, as an illustrator from home to supplement the household income. David enjoys his gadgets and invests what little money he has left into various pieces of electronic equipment, very much to the disapproval of Louise, as her priorities are naturally placed elsewhere. Nevertheless, David did concede to purchase the wireless baby monitor which will, according to the label, interoperate with their smart home system. The instructions themselves are quite simple: "Place the unit into an available wall socket in the child's bedroom and switch-on." The unit registers itself within the smart home environment and offers David and Louise an audible confirmation and a further opportunity to test the unit ensuring the device has set itself up correctly. Using a visual guide on the smart home system touch screen monitor, Louise confirms to Nora that the family room, kitchen, master bedroom and en-suite are the areas of significant importance where she should hear murmurs or whisperings from Daisy's bedroom.

It's 7:30am and David has just finished his breakfast and is ready to leave for work. As usual, David is very forgetful before he leaves for work in that he routinely forgets to take various items that he needs. "You do this every day," Louise says intoned with disbelief. Much to her frustration, she finds herself attempting to locate David's car keys while he puts on his jacket. The smart home system supports a unique feature called *KeyFinder*† where the car remote control is also registered within the home environment. After attempting to locate David's keys for the last few minutes, she concedes to locating them through Nora. Standing in the kitchen Louise walks to the front panel of Nora's touch screen monitor, and abruptly says, "Nora!" With a reassuring "beep" Nora acknowledges that she has heard Louise and lights up the screen where Nora presents Louise with several options, one of which is the KeyFinder function. Nora audibly notifies Loiuse that the keys are in the "downstairs bathroom" and like a little boy, David excitedly runs to the bathroom to retrieve them. Whilst holding the keys up to his face he shakes them and asks, “How did you get in there?” He turns to Louise and says “Thanks, love. What would I do without you?” The manufacturer of the car remote control unit collaborated with the car manufacturer where they both agreed a considerate function that allowed the remote control device to recharge its battery whilst it remained in the car ignition; in turn, it avoids the inevitability that the battery would die and Louise would never be able to find her husband’s keys. In addition to David’s briefcase, which only contains his sandwiches, he also retrieves his notebook and *FreedomPhone*.[†] We can all assume here that David’s notebook should be big enough to find and, of course, his FreedomPhone is always placed alongside his notebook in its desk charger.

Working with technology

The phone itself is a combination phone, in that it operates as a cordless handset within the home environment and is able to operate as a cellular phone when taken out of the home. It intelligently determines which particular environment it should be working within and, as such, seamlessly roams between wireless access points that have been deployed within the home or through the cellular network when away from the home. A proximity unit and signal strength indicator assists the device when determining context. The phone itself will attempt to remain connected to a wireless service, as opposed to being connected to the wider cellular network, as the cost of operating a phone through *Voice over IP* (VoIP) has plummeted due to the proliferation and increased growth of compatible products; undoubtedly budgetary considerations will always spur a new trend. To accommodate this overwhelming demand, New Jersey and elsewhere in the United States, has witnessed an increased deployment of wireless hotspots over the last eighteen months. Additionally, the car ferry service that David takes from New Jersey to New York offers a wireless service. The network operators are feeling the pinch in that they have observed a decreased revenue stream since the launch of the *FreedomNetwork*.[†] In an attempt to overcome these shortcomings, many operators have decided to launch their own compatible service alongside the FreedomNetwork, as well as offering bundled products luring existing customers to their networks. Many consumers using the product have embraced the simplicity in which they experience the ability to move from one environment to another using a single device. The phone will also transparently move between services depending upon the availability of a service; for example, if David operates his phone in an area that has a poor wireless coverage it will seamlessly transfer its connection to the cellular network without any notable degradation in voice quality. Another feature afforded with the FreedomPhone is its unique self-awareness function in that when it behaves as a cellular phone, the FreedomNetwork automatically assigns a unique cell number (David’s cell number). Similarly, when the phone is placed within the home it behaves as a cordless telephone and the home telephone number is assigned. Any cell calls that David receives will now be forwarded to the home phone, although David can switch this function off if he desires. The FreedomNetwork also offers David an answering service for his cell number if he has chosen to disable the forwarding service. The collective functions offered with the FreedomPhone enable Louise to continue using the home phone; likewise, Louise is also able to use the FreedomPhone product away from the home using another handset, as there are a minimum of three units with the FreedomPhone package.

Before entering his car, David places his briefcase and notebook in the trunk and as he opens the car door, he offers Louise and Daisy a final farewell. In the car he places his FreedomPhone in its placeholder within the vehicle. The car has now assumed responsibility for making and receiving calls where David can accept a call from his steering wheel, and using a series of voice commands, he can also make outgoing calls safely. The car itself is also equipped with a *Global Positioning System* (GPS), which is nowadays typically fitted to most standard vehicles. The system offers navigation assistance to David where typically he likes to avoid many of the traffic problems, but an additional benefit enables Louise and Daisy to track his progress to work on the *WhereAmI*† system. Holding Daisy, Louise closes the front door as David begins his daily journey and engages the WhereAmI function; all monitors within the home visually display David's progress.

David arrives at work around 8:45am and accesses the building's secured parking beneath the offices of his department. Using the *KeepSafe*† function, the barrier to the parking area wirelessly detects David's car, which lifts and allows him to drive in. The KeepSafe application is fitted to his car (as an option when the company purchased his vehicle) and in addition to this, he also uses a KeepSafe smartcard that permits him entry to the building's elevator, as well as other secured areas around the building. The premise of the KeepSafe ethos and its other range of products is that you become increasingly aware and associate capability with an iconic reference; for example, on entering the building David would have recognized the KeepSafe logo on the barrier. Similarly, he could have parked anywhere that supported the KeepSafe scheme. The KeepSafe manufacturer has worked extremely hard with widespread marketing through newspapers and TV, and has cooperated extensively with a myriad of manufacturers. As such, over a five-year period, consumers are now beginning to recognize that the KeepSafe-enabled range of products, transparently enable a host of applications by proximity, but most importantly, function is enabled through consumers' intent. You may recall in Chapter 4, *Can we Confidently Rely on Wireless Communication?* where we discussed the possibility of enabling intelligent connectivity through consumers' intent. In fact, David often recalls amusingly how he used to perform a device discovery with his cellular phone to connect to his headset. Nowadays, he simply brings the devices together and they become connected using the *KeepConnected*-enabled range of products, which is manufactured by the same company.

Entering his office, David places his notebook (KeepConnected-enabled) into the docking station and uses his smartcard to automatically log him into the company's network and services. He also places his FreedomPhone into the desk charger, which now behaves as his office phone, as the company purchased the FreedomPhone Business range. It essentially means that David's FreedomPhone is assigned an office number, in the same way it was assigned a cell number. Similarly, all cell calls are forwarded to David's office number. The KeepSafe manufacturer is currently reviewing and extending its product range for a variety of new applications, to include home and vehicle entry, but many technologists deem this to be unsafe as individuals regularly lose their smartcards.

Living with technology

At home, Louise is clearing up after breakfast and wishes to spend some playtime with Daisy; she is also reminded that she has to complete several illustrations as her deadline is looming. Louise has positioned her desk adjacent to David's as occasionally they will sit and work together over the weekend. The family room extends into the dining area, but to a large extent they primarily use the dining area as a study, since the kitchen is large enough to house a dining table. Louise has a desktop PC, which takes a more permanent position on her desk and she is wirelessly connected to the home system. As she sits at her desk, Daisy plays on the floor next to her where one of her favorite toys is her *BouncingTV*.[†] The BouncingTV is a childproof TV unit that can be thrown against a wall and it won't break – these are the claims made by the manufacturer. Anyway, the TV unit is a touch screen device that Daisy can interact with. Although, being a one-year-old child it is doubtful that she is aware of the fact that her interaction is indeed causing an effect. Nevertheless, she is incredibly excited in that her constant bashing of the durable touch screen monitor is causing various visual and audio stimulation to emanate from the TV unit. Occasionally, Louise will observe Daisy pausing her interaction with the TV while seemingly she absorbs the TV content; a few moments pass before Daisy resumes her apparent interaction. The unit itself is wirelessly connected to the home entertainment system, but the information supplied to the BouncingTV is specifically targeted for young children. Louise can use Nora to direct certain interactive TV programmes; similarly, Louise is also able to dynamically select programmes whilst sitting at her desktop computer. Louise spends a few hours at her desk and can visibly see that Daisy is increasingly becoming irritated, presumably the excessive bashing of her doll's head against the BouncingTV is an indicator; it usually confirms one of two things: she's tired or she's hungry. In selecting the latter reason, as default, she takes Daisy into the kitchen and places her into the highchair where she prepares herself and Daisy some lunch.

In the kitchen Daisy and Louise sit together eating their meal. Louise has switched on the kitchen TV where she can preview her illustrations; she needs to preview them and ensure that ultimately she's happy before submitting them to press. Using the TV remote control she can preview each illustration, essentially moving forward and backward at her own convenience. Ordinarily, Louise's day seems to run smoothly and without interruption; she now retires to the family room and spends that promised quality playtime with Daisy.

Moving swiftly through David's work day he gazes at his watch to discover that it's already 5:20pm. David is a creature of habit and he routinely calls Louise to let her know that he's leaving. "Okay, honey – I'll start dinner," she says in eager anticipation of his return home. Louise switches on the WhereAmI system allowing her to watch David's progress, as more often than not he encounters traffic problems and the evening meal typically becomes overcooked. With such impeccable management and timing skills Louise prepares the evening meal whilst looking after and feeding Daisy. It's 6:30pm; David arrives home and is greeted by Louise, "How was your day, honey?" David places his briefcase by the door and begins to remove his jacket, "It was okay, same old thing: what's for dinner?" he asks. Lifting his notebook from its case, David places it onto his desk along with his FreedomPhone where he hears Louise announce, "Your favorite! Keep an eye on Daisy for me, please."

David enters the kitchen and pecks Louise on the cheek and retrieves Daisy from her highchair, "How was your day, beautiful?" David returns to the family room and places Daisy onto the rug in front of the TV where he places himself onto the sofa. He offers Daisy a few toys and then picks up the remote control unit and begins to systemically "hop" through the various cable channels until he arrives at a channel that satisfies his visual need. Meanwhile, Louise is in the kitchen concurrently observing Daisy and finishing off the evening meal. It is clear that David and Daisy are individually lost in their own worlds in the family room. In the corner of her eye she can see the kitchen TV where the constant changing of channels is increasingly vexing her: "Choose a channel!" she screams, "Okay, I'm just looking." David stops his channel hopping and, feeling reprimanded, places the remote control down. The remote control unit is a similar dimension to that of a *Personal Digital Assistant* (PDA) and on it he can preview any channel on the remote control unit before finalizing his option with the home entertainment system. David nervously looks over his shoulder and asks Louise "Will dinner be long?" whilst furtively retrieving the remote control unit; he ensures that Louise isn't visually interrogating his subtle channel searching, which has now resumed on the remote control. "Won't be long now, honey," she says totally oblivious to his continued search. Still content and persistent, David resumes his search for the ultimate channel now in isolation and whilst, most importantly, remaining inconspicuous to Louise. The remote control unit is an integral piece of equipment that was initially supplied with the new build property and part of the smart home system. In any home the entertainment aspect is of crucial importance and, as such, the home is an experiential medium in which audio and video can be streamed to any or all of the rooms within the home. The cable company offers the interactive service supplied from a central cable unit where multiple rooms can individually choose to view a particular channel.

After sifting through over one hundred channels three times, David becomes increasingly annoyed as he can't find anything to satisfy his visual gratification. He resorts to sitting in the study area of the room where he had set-up his notebook. Most poignant of this configuration is the ability to roam from office and home seamlessly. There was a time, David recalls, where many consumers experienced the inability for a notebook computer to auto-configure in its environment. Nowadays, David doesn't need to interact with his notebook to configure the environment in which it finds itself; he erects the notebook monitor and switches it on. The notebook itself is self-aware and automatically recognizes the environment in which it finds itself and becomes ready to use; the notebook informs David, "I'm home." Sitting at his desk, he starts to mindlessly surf the Internet. The notebook, naturally, is wireless-enabled and auto connects to a host of peripherals on his desk, such as the large monitor, mouse and printer. Nora is able to allow David to carry his notebook to any room where he would still remain connected to the Internet. Similarly, he is also capable of using the printer from any room.

At 7:10pm David is reprieved from his boredom and with Louise and Daisy they all sit in the kitchen to enjoy their meal. Daisy is placed into her playpen, allowing David and Louise to mull over their respective day. Having both finished their meals David offers Louise, much to her surprise, assistance in the kitchen and they both begin to clear away the evening meal. Most unexpectedly, Nora announces, "There's someone at the door." David and Louise both stare at each other as neither of them were expecting anyone. Louise moves to Nora's touch screen monitor and selects the *PreviewVisitor* function, only to discover that it's her grandmother, Emily. During the preview function, Nora is able to convey any audio from the door to the rest of the home system, typically to the integral speaker system in which the preview function was activated, "I know you're there," says Emily. Louise, throwing down her kitchen towel, walks to the front door to let her grandmother in. "Hello, Gran – this is unexpected." Brushing past Louise, Emily enters the house and makes herself comfortable in the family room. "Can I get you anything, Gran?" Placing her handbag down onto the floor she says, "Sorry dear, I'll have a cup of tea, I won't be long; I just wanted to see my great granddaughter." Emily is in her late eighties, but quite remarkably remains fit and well, as she insists on walking as much as possible – taking in that fresh New Jersey air no doubt! Her only grievance is that recently she has become deaf and has to use a hearing facility to enhance the voice quality in general conversation. The equipment is discreet and to a large extent most people are unaware of her condition. In fact, David and Louise's home system supports a function, which will pick up voice-specific audio within the room and interacts with Emily's hearing system allowing her comfortably to hear any conversation. An hour-or-so passes and Emily thanks David and Louise for their impromptu hospitality. Looking relieved, David whispers to Louise "It's about time she left." Every time Emily visits he forgets that Nora is capable of enhancing voice communication and unfortunately, Emily hears the whispering and disapprovingly acknowledges David's remarks "Yes, I know when I'm not welcome." David grumbles under his breath "Nora," where dutifully she illuminates her touch screen monitor awaiting instruction.

Emily doesn't live too far from David and Louise's house and are both confident that Emily will return home safely. With such a healthy pension, working over fifty years, Emily was able to purchase and invest in a personal alarm system and equipping part of her home with a smart home system (part of the KeepSafe range of products). Emily originally purchased her home without the extensive home system that David and Louise purchased and was adamant that she didn't need to rely on technology. Nevertheless, Emily's home system is a considerable cut down version of the advanced home system that David and Louise purchased in that it doesn't have the convenient TV remote control system and so on, but she did concede to adapting her home to accommodate the invaluable hearing system. In fact, Emily purchased the home without any inherent technology and it was offered as an upgrade to the house. It was seamlessly integrated and installed with minimum inconvenience. The particular estate in which they occupy has an extensive wireless hotspot service, which allows Emily to make use of a wireless pager. She wears a *KeepWell*[†] pendant around her neck that when engaged will notify her next of kin, but most importantly will notify the emergency services that she is in danger or feeling unwell. The pager system is capable of identifying the individual who alerted the authorities; location, address, name and other contact information is passed on. Similarly, when she is at home and feels disturbed or restless she may call assistance to her home.

It's 11:30pm and David and Louise retire to bed knowing that the alarm will sound at 6:00am and no matter how hard David hits the snooze button there is no denying that a new day must start. Much to her annoyance Daisy was put to bed earlier in the evening around 8:00pm and characteristically protested at her early departure from the family lounge. David and Louise together ensure all the doors and windows are locked in the house before going to bed and the security system acknowledges that the house is secure. The security system is set to "bedtime" where all the occupants are now retiring and the system automatically sets the intruder alarm, as well as feeding the audio for the baby monitoring system through to the master bedroom and en-suite. Entering the bathroom, David and Louise routinely stand adjacent to their "his and her" wash basins to clean their teeth. Louise naturally spends a little longer at her basin and uses various products to remove her make-up, whilst exfoliating her skin. David, after finishing cleaning his teeth, turns to Louise and attempts to kiss her lips while trying to avoid the various products she's used on her face. Turning to the bedroom, David wipes his lips and runs to the bed where he takes a leap and lands in the centre bouncing up and down several times; pondering for a moment and declares "I'll check on Daisy." Entering Daisy's bedroom he's careful so as not to disturb her, but as he peers into her cot she opens her eyes wide; she smiles at him and he says "Hey baby, sleep now. I missed you today. You're the best beautiful – yes, I know your mum has her moments, but I do love you both very much." Unknown to David, the fallible baby monitor is unable to distinguish between daddy's and Daisy's whisperings.

A subtle moment of technology enhancing the quality and experience of life.

Summary

- We continue to blindly thrust wireless technology into consumers' faces and expect them to know everything.
- We should move beyond a necessity to educate and make assumptions about our audience.
- Instead, let's infuse an expectation of untethered experience.
- It's only recently that advocates of wireless technology have realized that consumers need an *out-of-the-box* experience.
- If you purchase a new cellular phone today, for example, it is indeed an out-of-the-box experience, as you simply remove the packaging, insert the battery and SIM card; once you switch it on there is no configuration or set-up, you just automatically become connected to the network operator's service.
- The marketers' incentive should not be just an argument of "well, we can;" nor, should it be a contest between manufacturers.
- More importantly, product development should be based solely upon consumers' needs and expectations.
- Consumers may be prepared to levy a budget and benefit from such products if a quantifiable list of expectations are met.
- We should enforce a second nature where the technology itself knows how it should work, something along the lines of self-awareness and self-configuration.
- Technology should remain supportive and incidental.

Notes

[*] A fictitious super computer that was created by a pan-dimensional intelligent race of aliens. It existed only in the world of the *Hitch Hiker's Guide to the Galaxy* by Douglas Adams and its sole purpose was to ultimately answer the meaning of life, the universe and everything (incidentally, the answer was 42).

[†] The reference to this product in this chapter or elsewhere in this book remains fictitious and any reference made to an actual product is purely coincidental.

Part Two

A Proprietary Approach to Developing Wireless Applications

This page intentionally left blank

6

An Introduction to the Notion of Proprietary-based Wireless Application Development

With an unrelenting onslaught of non-profit standardization organizations each with an objective to steer and drive the future of their respective technologies, we have to reluctantly admit to putting up the white flag, and confessing: it's somewhat difficult to keep up! The countless acronyms, *three letter abbreviations* (TLAs), compliance and interoperability specifications can only lead to confusion and boredom. Equally, proprietary solutions are guilty of their TLAs; it's evidently unavoidable, but more often than not they offer a solution that is ready and works. At last we can actually envisage in our four-year roadmap a product being physically developed, affording us flexibility and opportunity to place our product into the big wide world of consumerism.

With our eager desire to deploy the latest wireless-enabled products, manufacturers conduct endless research and through this, begin to glean an understanding of the multitude of wireless technologies available to them. In sifting through the numerous specifications and becoming aware of the standards bodies that govern them, and of course the constraints and expectations to abide by a myriad of rules and regulations, it is unequivocally a daunting prospect. Let's think out of the box. Manufacturers, after all, are not bound by the norm; if their product does not have to interoperate with the mass market and your product is unique, why not create or select a proprietary wireless technology that suits your application?

Case Studies

This chapter unpretentiously whets your appetite, as to what is to follow. We examine several companies (see Table 6.1) who have taken their own steps in creating a wireless technology, not necessarily to compete with the greater market, but merely to serve a market that needs a wireless solution today.

Admittedly, there are numerous companies developing proprietary solutions, although with limited time and space we take an opportunity to highlight three successful companies that have succeeded in delivering exactly what the customer wants.

Table 6.1 *A selection of companies that have delivered proprietary wireless technologies*

Company	Chapter	Description
ZenSys	Chapter 7	An Open Standard for Wireless Home Control
Cypress	Chapter 8	Cypress Semiconductor: Introducing WirelessUSB
Aura	Chapter 9	Aura Communications Technology: Creating the Personal Bubble

7

ZenSys: An Open Standard for Wireless Home Control

The notion of a talking refrigerator may have haunted some of us for many years. Indeed, the thought of your home being an intelligent entity can only induce a fear of the unknown. Equally, it has to be somewhat unnerving when your fridge informs you that you're out of milk. It clearly knows more than you do and paranoia surely sets in. You become increasingly aware that your home equipment is having a secret conversation – you begin to make eye contact with your equipment; visually interrogating it, and then can only speculate on the conversation. Moreover, you feel a pair of electronic eyes watching your every move, just like the photograph of your mother-in-law above the fireplace. Perhaps we are being a little hysterical! Admittedly, the photograph of your mother-in-law indeed follows you around the room, but as for your white goods and other home equipment developing a Freud-like "Id," void of ego, that's a long way off. On a more serious and relevant theme, the reality indicates that there *is* a growing demand from consumers to equip their new homes with some sort of home automation. In fact, the high-end property market is being fitted with such systems as standard. Home security, comfort and control, within and away from the home, are a number of escalating factors that have founded the way in an increased demand for such systems within the home environment.

We can easily imagine the high-end property market enjoying the benefits of home automation, as the property price often reflects the value-added benefits. But to achieve global market penetration for more modest homes would require a technology that was low-cost. Equally as important, is low-power, as most homes would not want to see a significant increase in their utility and service bills. Moreover, you don't necessarily want the encumbrance of continually repairing your home automation equipment; therefore you can envisage utilizing a self-repair mechanism which, naturally, would prove to be advantageous.

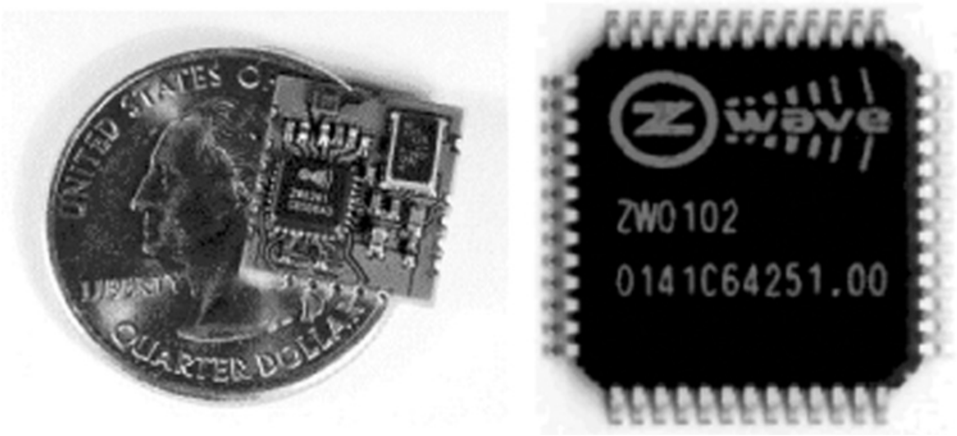


Figure 7.1 *The Z-Wave module has been designed for applications such as home control and comprises a complete hardware and software platform to include a microprocessor, memory, RF circuitry and a software protocol.*

Does this sound like science fiction? No. In fact, to accommodate this growing demand, ZenSys (www.zen-sys.com) have created a wireless home control system that assures us of nothing more than a safe and secure environment, in essence matching the core foundation for the key factors we have already identified. What's more, they have developed a low-cost, low-power and self-healing solution with their Z-Wave silicon and protocol products, see Figure 7.1 and Figure 7.2. There are no talking refrigerators

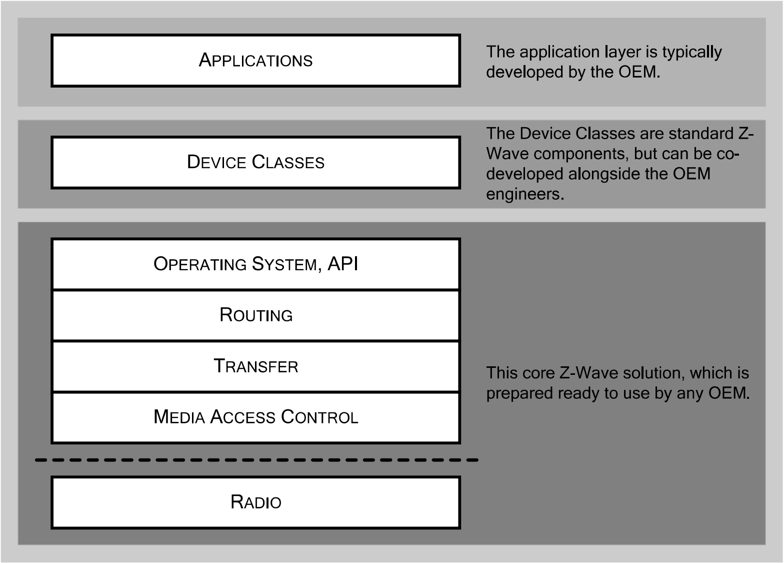

Applications
The application layer is typically developed by the OEM.
Device Classes
The Device Classes are standard Z-Wave components, but can be co-developed alongside the OEM engineers.
Operating System, API
Routing
Transfer
Media Access Control
Radio
This core Z-Wave solution, which is prepared ready to use by any OEM.

Figure 7.2 *The Z-Wave protocol stack where the complete system can be combined with the Z-Wave ASIC offering between 8KB and 18KB of application source.*

here, just home control, automation and security for all types of homes, irrespective of price and size. ZenSys' Z-Wave is a *Radio Frequency* (RF) based system that supports bi-directional communication and enjoys the benefit of *mesh* networking (more about this later). Before we continue to delve into the finer detail of the technology, let's take a look at the company's background and history.

Background

ZenSys was founded in 1999 and supports two headquarters across two continents: in Europe (Denmark) and the United States. With a mission to establish its Z-Wave technology as the de facto standard for wireless home control, it has already secured $14 million in funding for its silicon and module design with further investment to follow for its 300-series silicon. In a succession of catalogued milestones, ZenSys have secured a partnership with Intel creating a combined vision for the *Digital Home*, and have established over one hundred customers to include Leviton (www.leviton.com), Intermatic (www.intermatic.com), Cooper (www.cooperwiringdevices.com) and Honeywell (www.honeywell.com). Furthermore, in underpinning its technology as ubiquitous wireless connectivity within the home, ZenSys have formed a coalition, namely the Z-Wave Alliance, comprising approximately seventy-five members. Naturally, such a significant number of member alliances as strategic supporters will ultimately found the technology as a standard means for wireless home control. Inevitably, we will undoubtedly witness this solution becoming a standard technology within the home control arena where ultimately it is envisaged being placed in the relevant section in this book!

Enabling Wireless Home Control

We've undoubtedly experienced or have come across citations to the *SmartHome* furore. It's not a new concept; it's merely about belief, cost and greater simplicity. In our introduction to this chapter we touched upon the larger, expensive homes enjoying the benefits of home automation. In turn, the 80s and 90s witnessed an elite members' club of homeowners who could afford such technologies. Nonetheless, this doesn't necessarily bode well with a company's success and financial prosperity. To succeed in the wider market and to achieve greater market penetration a more cost effective affordable solution that is open to all is needed. Naturally, in a competitive industry, ZenSys is not alone in wanting to succeed with this global vision; other companies and/or standards, such as Cypress' WirelessUSB sensor technology and ZigBee are both offering and developing new alternative technologies (incidentally, we discuss

WirelessUSB in Chapter 8, *Cypress Semiconductor: Introducing WirelessUSB*, and ZigBee in more detail in Chapter 12, *ZigBee Untethered and Unlicensed*). Additionally, consumers, or more accurately home owners, don't necessarily want to undertake a four-year degree programme in technology to enable them to understand and use their homes. As such, the ability to intelligently interact with your home equipment is also paramount to its success and longevity.

We are inescapably aware of the need for low power and affordability, but we need to address issues of deployment and installation. Indeed, many solutions can be independently installed by the homeowner who may be confident in enabling their smart home technology; on the other hand, and arguably the majority of homeowners would not be as confident in installing such a system. We should not forget that ZenSys is primarily a company that provides a technology that affords its adopters to use its solution to develop home automation products. These adopters may provide an installation, deployment and support structure that allows homeowners to purchase a solution that matches their requirements and, thus, removes the need for them to undertake that four-year degree programme!

Enabling the Wireless Home Control Network

Manufacturers are often faced with decisions that will ultimately affect the future success of their products and personal success within the specific market arena they choose to dominate. Indeed, the potential number of applications available to a product developer is numerous and, in turn, only limited by their imagination. Products such as, light switches, camera surveillance, access control and, despite making light of the talking refrigerator in our opening paragraph, this notion is increasingly becoming a reality. The following discussion is concerned with a technology that enables a wireless home control network, in turn, resurrecting the infamous genre of smart home technologies.

The RF transceiver

It is always a good place to start with the radio. The premise of the radio transceiver is singularly the most important part of the success of any wireless product alongside a well-balanced and proportioned application base. The Z-Wave chip operates within two frequency ranges, namely 868.42MHz for Europe and the *Industrial Scientific and Medical* (ISM) 908.42 band for the United States. These two bands are well established within the industry, assuring us of reliability and offering a good radio range and, equally as important, affordability. Figure 7.3 illustrates the modest set of components

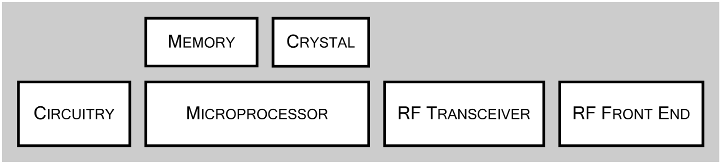
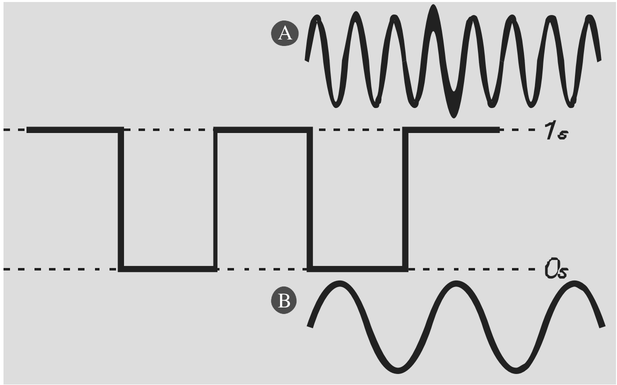


Figure 7.3 *The modest set of components that comprise the RF platform, in turn, assuring a reliable, cost effective, low power solution.*

that comprise the RF platform confirming a reliable, cost effective and low power solution. In combining these qualities, ZenSys can truly begin to secure and succeed in providing a ubiquitous wireless solution for the home.

The Z-Wave transceiver offers two-way communication and uses the *Frequency Shift Keying* (FSK) modulation spectrum shaping method. This particular scheme transforms two analog waveforms into the two binary states, *ones* (1s) and *zeros* (0s), as we illustrate in Figure 7.4. In the illustration the *A* waveform represents a high state where the analog sine wave will be converted to a one (1); and, conversely the *B* waveform represents a low state which is converted to a zero (0). You may recall the application of a modem, which performs a very similar function in that it takes the analog signal from the telephone line and converts it into digital signals for the computer to process; and vice versa, the modem converts the digital signals into analog signals to transmit back over the telephone line. ZenSys have not only simplified the selection of the RF components but have thought ahead about a platform and the generic availability of its components and its translation to assembly and production.

Figure 7.4 *The FSK modulation spectrum shaping method takes two analog waveforms (A and B) that represent each of the binary states, one and zero.*



Alongside this you have attributes such as cost and simplicity, which are crucial in producing a wireless home control solution as the sensitivity in cost of home control products is paramount and, over a relatively short-term period, needs to penetrate a wide and diverse consumer market. Similarly, the impact of power consumption is evidently important within the home environment and the RF platform and its intrinsic component base seem to appease the dichotomy of consumption versus reliability. And finally, the component base is sufficiently small enough, allowing the simplest of integration into many existing home products, as the small form factor size has a negligible impact on the overall product platform.

The mesh networking topology

The foundation upon which the Z-Wave topology finds itself is primarily based on a mesh network, as illustrated in Figure 7.5. As the dictionary definition describes, a mesh is a web or lattice structure that is interconnected. The advantage prescribed by such a structure is that there is no server or host machine required and, as such, if a node becomes unstable or dies within the mesh, then the entire system does not fail. It follows a self-sustaining ethos, as we earlier described. Additionally, the exposure or range covered by Z-Wave logistically exceeds most personal-area technologies, as a mesh can cover, for example, an area from five to several hundreds of meters (the number of nodes is restricted to 232, although this may be extended through multiple mesh networks). The distribution and number of nodes in an environment should also

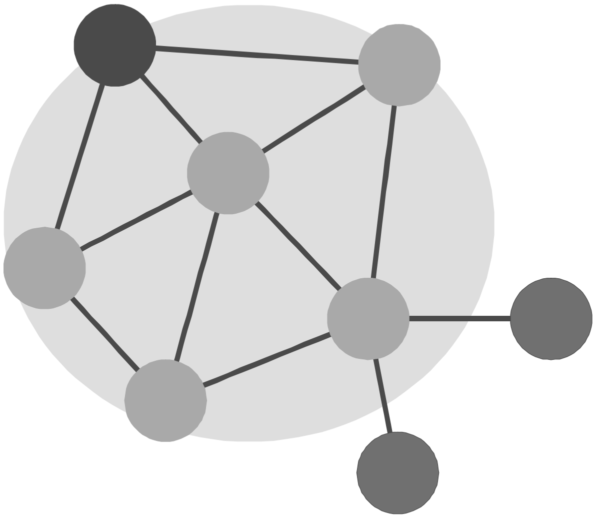
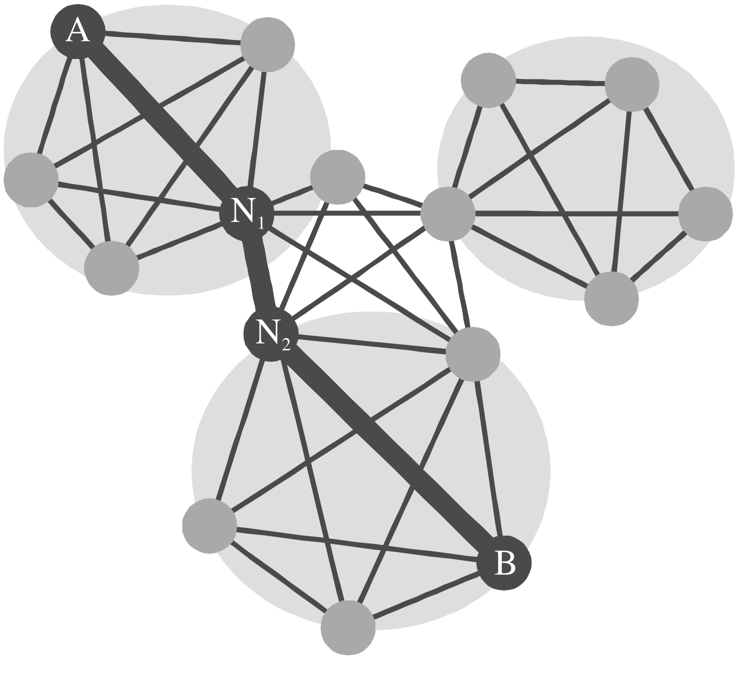


Figure 7.5
The mesh network topology forms a web of interconnected nodes.

be kept to a minimum, as naturally the cost is conversely greater if a larger number of nodes are required. The use of a *Source Routing Algorithm* (SRA) provides an effective balance between the proposed number of resources (nodes) and the overall network size. The SRA, like a driver of a bus knowing his/her route particularly well, will package the route and destination information within the header of a payload. When the payload reaches each node within the route the header information is updated to reflect the journey already traveled. As each node is interconnected, a message can be sustained across the network until the destination node is reached. In a similar fashion this can be likened to someone requesting a fellow diner to pass the salt across a table of forty or so people; the salt is passed down the table until the person who requested it, receives it.

We illustrate in Figure 7.6 a message being transmitted from node *A*, which needs to reach node *B*. The formation of the mesh network enables node A to traverse the message through nodes N_1 and N_2. Incidentally, if N_1 was unavailable, then the mesh network would facilitate the use of other available nodes to route the message accordingly. The mesh network is not restricted to fixed nodes either; a node can occupy a portable device affording the technology versatility, in turn, enabling devices to roam within a mesh network. The relatively short data payloads create a low latency of approximately 200ms or more in data transmission where an available 9.6Kbps bandwidth seems to be sufficient to maintain a satisfactory communication medium. However, in

Figure 7.6
The controller node A wishes to pass on a message to the slave, node B and uses the routing slaves, nodes N_1 and N_2 to relay the message.



the 200 series ASICs offered by ZenSys the data transmission has now been increased to 40Kbps and, as such, the latency is further reduced, that is, lower than 200ms. It seems that a common practice is used within the developer community. If a device does not respond within this 200ms window, then generally, consumers are led to believe that the device has failed. For example, if a user presses a button on a remote device to turn on a light and the device fails to respond within the latency window, then the user will press the button again, undoubtedly turning his/her living room into the state of the art strobe effect lighting. The dynamic and flexible behavior of the Z-Wave technology can be attributed to the three categories of node types, namely *controllers*, *routing slaves* and *slaves*. The combination of these types of nodes can arbitrarily be dispersed in any environment, although, as we have already mentioned, the distribution should be made conservatively. The topology of the Z-Wave technology enables devices such as dimmer switches, thermostats, movement sensors and so on to behave as repeater nodes, so a conservative approach may not necessarily be strictly adhered to. The configuration of these devices is subject to the environment in which they need to be placed and, of course, the application of which they serve. For example, there will be nodes that initiate communication with other devices; these nodes will require a controller or routing slave protocol. In Figure 7.6, node A would be described as a controller node as it initiated communication; whereas a node that needs to initiate communication with a well-defined subset of nodes is based on a routing slave protocol. Similarly, node A in our illustration could also assume this behavior. Finally, a node that does not need to initiate communication but merely reacts to other requests from other nodes in proximity is based on the slave protocol. N_1 and N_2 will behave as routing slaves, as they need to initiate communication with one another to convey the message from node A. In revisiting our illustration (Figure 7.6) node B would be described as a slave as it simply reacts to the instructions that have been conveyed by node A through nodes N_1 and N_2.

Self-organization, self-healing and ease-of-use

The controller and routing slave nodes possess adaptive characteristics, in that if a node has been deployed into a portable device it has the capability of dynamic localization and the support for re-discovery of mobile nodes within the mesh network environment. The controller node types enable easier installation, as they also have the ability to manage and to self-organize; this metamorphic behavior may occur when a *Static Update Controller* (SUC) node assumes the responsibility of a *SUC Id Server* (SIS). The set of parameters which prescribes such functionality are distributed to other controller nodes. Each node within the mesh network has the ability to learn of its neighbor by requesting information. This behavior supports our paranoid notion that equipment in the home is indeed having a seemingly private conversation.

Nevertheless, every node informs the SUC of its availability, as the SUC node is always listening. This self-organizing behavior is of particular importance, as a user does not need to know how each node intercommunicates. Instead, the SRA assures the initiating nodes that all destination nodes can be reached. We have already touched upon the ability of the dynamic behavior in which the mesh network behaves if one node becomes unavailable for whatever reason. This ability to adapt in its own environment is classed as self-healing and, in part, the SRA denotes the defective node unavailable from its route. The node itself may be operational; however, environmental conditions such as metal objects may cause fluctuations or unreliability in the radio link. The process of self-healing encourages a supportive environment and offers no excuses for the technology to continue from sustaining normal operation.

A different kind of class

The software behind the protocols and algorithms is based upon various classifications. These classifications relate to specific roles and behaviors within the mesh system, as we have already touched upon, although the behavior within the system remains dynamic. In this section we shall introduce specific characteristics within the software architecture that maintain the ability to create a cohesive and well-balanced home control environment. But first, we should remind ourselves that ZenSys and its Z-Wave technology is a means by which other manufacturers base their home control products upon. As such, with an increasing number of manufacturers adopting the technology and the opportunity for multiple product interchange, Z-Wave products will ultimately need to *interoperate*. You may recall from Chapter 4, *Can we Confidently Rely on Wireless Communication?* that we discussed the importance of interoperation and how the definition of a protocol stack and its peer-to-peer communication afforded successful interoperation. We have already introduced the fact that ZenSys have consorted with a number of companies and formed their own alliance with an approximate membership of over seventy-five members. It is clearly evident that the technology increasingly needs to interoperate with multiple manufacturers or vendors and, as such, ZenSys have created an underlying protocol stack with specific roles and responsibilities to meet the unique characteristics of the Z-Wave philosophy. In Figure 7.7 we illustrate the conceptual representation of the available applications from Z-Wave's wireless home control network. The inclusion of these diverse applications is a constant reminder that one vendor may develop the lighting products whilst another may develop the security application; nevertheless, products from both manufacturers will need to interoperate.

The premise of the technology is to establish basic, generic and specific device classes to achieve the identification and ultimately responsibility of a node within the

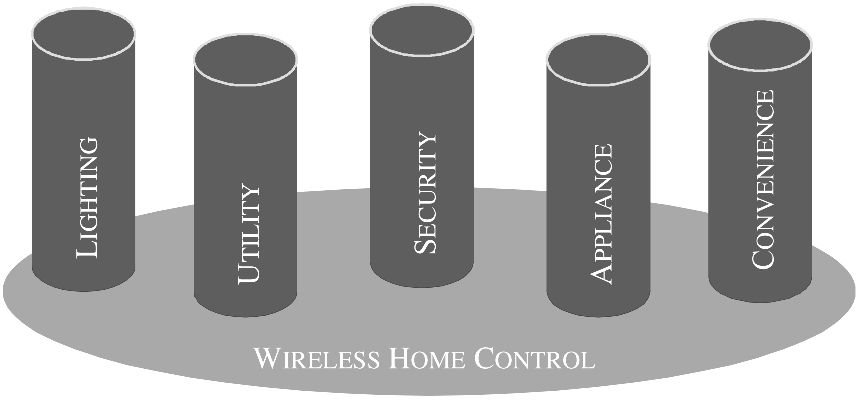


Figure 7.7
A conceptual representation of the Z-Wave wireless home control network encompassing the potential application areas.

home control network; each classification further prescribes a number of unique attributes. Furthermore, communication is achieved by issuing a series of commands, which are organized into a number of command classes. The grouping of these commands is pinnacle in establishing the functionality of a device. At the heart of a device the generic device class forms the basis of primitive functionality and is extended with other classes to create additional or recommended classes that further define its behavior. In Figure 7.8 we illustrate the generic architecture of Z-Wave enabled applications and its underlying class structure.

A device inherently contains functionality that comprises a logic grouping of the available basic commands. The device will contain the set of mandatory commands in addition to the selection of appropriate command classes. It is this variation of selecting what to integrate into the product that offers diversity from one vendor to another, but of course, each vendor still achieves interoperability, as the behaviors are all inherited. The command structures relate to the specific implementation of wireless home control, such as lighting, automation, control and so on, where the combination of device classes support the basic command class as a default requirement. It contains further instructions on how to map specific commands to support the device itself, as we illustrate in Figure 7.9.

Conclusion

ZenSys have such audacity in pushing a technology into a market that has seen a surge of other similar technologies achieve similar objectives. It *can* confidently proclaim affordable, reliable and power friendly technology that unites a myriad of wireless

Figure 7.8
The generic perspective of Z-Wave enabled applications and their underlying device structure.

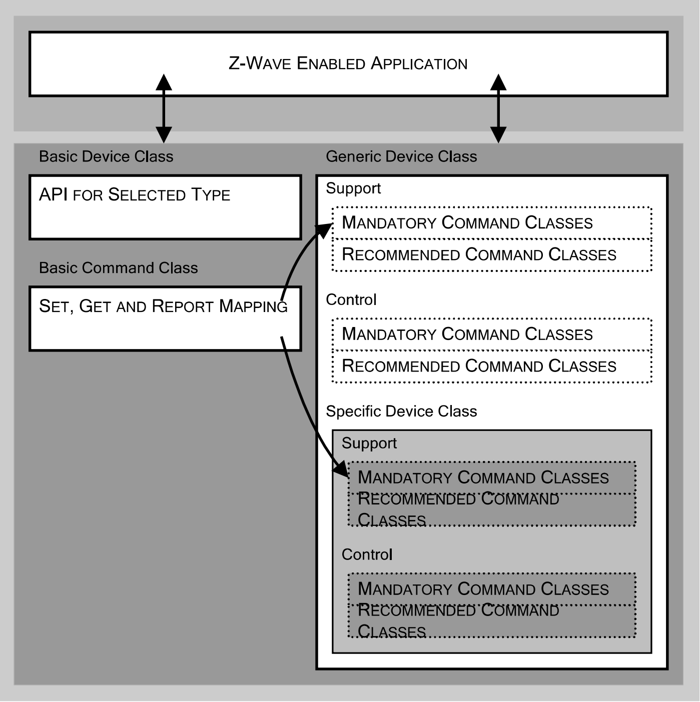
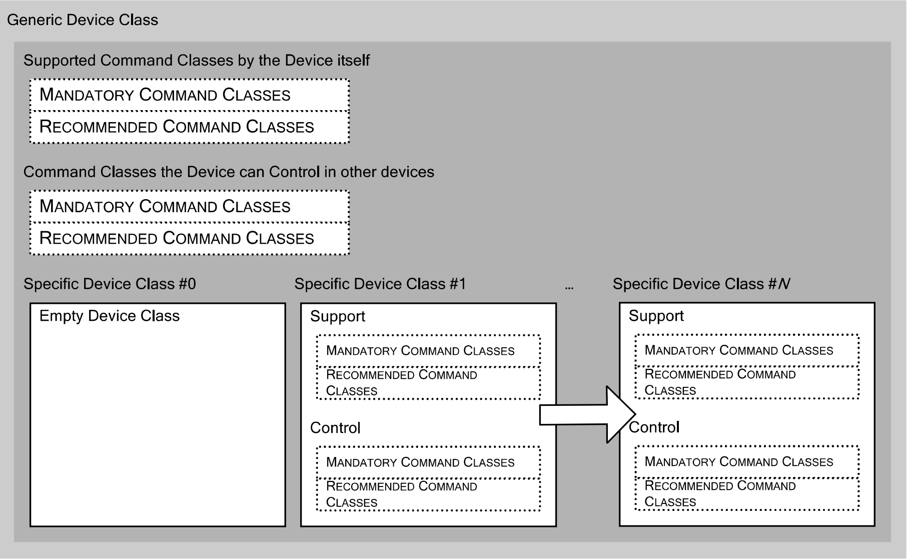

Z-Wave Enabled Application
Basic Device Class
API for Selected Type
Basic Command Class
Set, Get and Report Mapping
Generic Device Class
Support
Mandatory Command Classes
Recommended Command Classes
Control
Mandatory Command Classes
Recommended Command Classes
Specific Device Class
Support
Mandatory Command Classes
Recommended Command Classes
Control
Mandatory Command Classes
Recommended Command Classes

Figure 7.9
The formation of specific and generic device class structures.


Generic Device Class
Supported Command Classes by the Device itself
Mandatory Command Classes
Recommended Command Classes
Command Classes the Device can Control in other devices
Mandatory Command Classes
Recommended Command Classes
Specific Device Class #0
Empty Device Class
Specific Device Class #1
Support
Mandatory Command Classes
Recommended Command Classes
Control
Mandatory Command Classes
Recommended Command Classes
...
Specific Device Class #N
Support
Mandatory Command Classes
Recommended Command Classes
Control
Mandatory Command Classes
Recommended Command Classes

home control products. It's a proprietary solution, enabling would-be developers to develop and create products now! A final thought though should be given to the ZigBee Alliance (and others): while these collective companies strive for similar aspirations, ZenSys will ultimately need to stay one step ahead. Collaboration with many other companies and having the ability to demonstrate that their solution does work and indeed is already installed in many homes will surely help in distinguishing them from any competitor, as ZigBee is relatively still in its infancy. And, inevitably, the process of empowering many manufactures with Z-Wave technology will undoubtedly lead to a more formal, perhaps slower, process of creating Z-Wave technology enabled products, as each product will need to interoperate successfully. Additionally, ZenSys will need to prepare a host of added value benefits and services that will, in time, brandish the technology of its nearest competitor as dilapidated and obsolete.

Summary

- The notion of your home being an intelligent entity is increasingly becoming a reality.
- The high-end property market enjoys the benefits of home automation, as the property price often reflects the value-added benefits.
- To achieve global market penetration for more modest homes would require a technology that was low-cost.
- Low-power is an important consideration, as most homes would not want to see a significant increase in their utility and service bills.
- Additionally, you don't necessarily want the inconvenience of continually repairing your home automation equipment.
- ZenSys have created a wireless home control system that assures us of nothing more than a safe and secure environment.
- ZenSys have developed a low-cost, low-power and self-healing solution with their Z-Wave silicon and protocol products.
- ZenSys' Z-Wave is an RF based system that supports bi-directional communication and enjoys the benefit of mesh networking.
- ZenSys was founded in 1999 and supports two headquarters across two continents: in Europe (Denmark) and the United States.
- Z-Wave is attempting to establish itself as the de facto standard for wireless home control and has already secured $14 million in funding.
- ZenSys have formed a coalition, namely the Z-Wave Alliance, comprising approximately seventy-five members.

- With such a significant number of member alliances as strategic supporters will ultimately found the technology as a standard means for wireless home control.
- We've undoubtedly experienced or have come across citations to the SmartHome gossip.
- It's not a new concept; it's merely about belief, cost and greater simplicity.
- The 80s and 90s witnessed an elite members' club of homeowners who could afford such technologies.
- Although, this doesn't necessarily bode well with a company's success and financial prosperity.
- To succeed in the wider market and to achieve greater market penetration a more cost effective affordable solution that is open to all is needed.
- ZenSys is not alone in wanting to succeed with this global vision; other companies and/or standards, such as Cypress' WirelessUSB and ZigBee are offering and developing new alternative technologies.
- Home owners don't necessarily want to undertake a four-year degree programme in technology to enable them to understand and use their homes.
- The ability to intelligently interact with your home equipment is paramount in its success and longevity.
- ZenSys is primarily a company that provides a technology that affords its adopters to use its solution to develop home automation products.
- Adopters may provide an installation, deployment and support structure that allows homeowners to purchase a solution that matches their requirements.
- The Z-Wave chip operates within two frequency ranges, namely 868.42MHz for Europe and the ISM 908.42 band for the United States.
- These two bands are well established within the industry assuring us of reliability and offering a good radio range and, equally as important, affordability.
- The Z-Wave transceiver uses the FSK modulation spectrum shaping method.
- This particular method transforms two analog waveforms into the two binary states.
- The foundation upon which the Z-Wave topology finds itself is primarily based on a mesh network.
- A mesh is a web or lattice structure that is interconnected.
- The advantage prescribed by such a structure is that there is no server or host machine required.
- If a node becomes unstable or dies within the mesh, then the entire system does not fail.
- The exposure covered by Z-Wave, logistically exceeds most personal-area technologies.

- The use of an SRA provides an effective balance between the proposed number of nodes and the overall network size.
- The SRA will package the route and destination information within the header of a payload.
- When a payload reaches each node within the route the header information is updated to reflect the journey already traveled.
- As each node is interconnected a message can be sustained across the network until the destination node is reached.
- A mesh network is not restricted to fixed nodes – a node can occupy a portable device affording the technology versatility.
- Short data payloads create a low latency of approximately 200ms or more in data transmission, although new ASICs provide better latency timings.
- An available 9.6Kbps bandwidth seems to be sufficient to maintain a satisfactory communication medium and again new ASICs offer greater bandwidth.
- The dynamic and flexible behavior of the Z-Wave technology can be attributed to the three categories of node types: controllers, routing slaves and slaves.
- The controller and routing slave nodes possess adaptive characteristics.
- If a node has been integrated into a portable device it has the capability of dynamic localization and the support for re-discovery.
- Each node within the mesh network has the ability to learn of its neighbor or may do so by requesting information about its neighbor.
- Every node informs the SUC of its availability, as the SUC node is always listening.
- This self-organizing behavior is of particular importance as a user does not need to know how each node intercommunicates.
- The SRA assures the initiating nodes that all destination nodes can be reached.
- The software behind the protocols and algorithms are based upon various classifications.
- Classifications relate to specific roles and behaviors within the mesh system.
- It is increasingly important for Z-Wave to interoperate with multiple vendors and, as such, ZenSys have created an underlying protocol stack with specific roles and responsibilities to meet the unique characteristics of the technology.
- The grouping of these commands is pinnacle in establishing the functionality of a device.
- At the heart of a device the generic device class forms the basis of primitive functionality and is extended with other classes to create additional or recommended classes that further define its behavior.

- A device inherently contains functionality that comprises a logic grouping of the available basic commands.
- A device will contain the set of mandatory commands in addition to the selection of appropriate command classes.
- It is this variation of selecting what to integrate into the product that offers diversity from one vendor to another.
- The command structures relate to the specific implementation of wireless home control, such as lighting, automation, control and so on.
- ZenSys have pushed a technology into a market that has seen a surge of other similar technologies achieve similar objectives.
- It can confidently proclaim affordable, reliable and power friendly technology that unites a myriad of wireless home control products.
- It’s a proprietary solution enabling would-be developers to develop and create products now!

8

Cypress Semiconductor: Introducing WirelessUSB

The *Universal Serial Bus* (USB) has been around for almost as long as the PC and the simplicity afforded by such a technology has perpetuated the notion of connectivity as a simple means of plugging one end into another – just perfect! As time has moved on the Microsoft Windows *operating system* (OS), as well as other popular OSs have moved on too, making life much simpler for the everyday consumer: you simply plug in your USB-enabled device and the OS takes care of it all: the software installation and associated device drivers. Nonetheless, the advent of wireless was expected to ease the transition from cables to a cable-free environment – after all, cables are cumbersome and awkward – aren't they? Are cables that bad? Do they continue to cause such grievances that we need to continue to untether them? We have, after all, come to master the trickery associated with the cable and the strange looking connector at its end, trying to visualize how this would connect to "my" device – surely this was the inception of infotainment, as you had the dichotomy of education accompanied with the amusement of pushing a square connector into a round hole? But then, to marry wireless with USB has to be genius. We are already familiar with a technology that has comfortably connected one device to another – and there's no getting it wrong as the connectors are transparent to any technophobe despite the insistent pushing of the square connector into the round hole! And, then you have wireless, a transparent medium which, when prepared to your taste, allows you to enjoy a seamless conversion to a cable-free table top. Take USB and a generous soupçon of wireless; now gently snip the cable away: there you have it, the perfect recipe for *WirelessUSB*.

Who'd have thought that the combination of such simple ingredients to make WirelessUSB would have been just as simple as that? Okay, maybe not. Nevertheless, Cypress Semiconductor (www.cypress.com) do have the right ingredients for WirelessUSB and it takes the form of a patent-pending, frequency-agile,

Figure 8.1
A look at Cypress' WirelessUSB solution, namely the PRoC WUSB LP flash programmable microcontroller with integrated 2.4GHz radio transceiver.

Direct Sequence Spread Spectrum (DSSS) offering a combination of low power, reliability and alleviating coexistence from a plethora of sources to include cordless phones, Bluetooth wireless technology and WiFi. The Cypress is a commercially available *Programmable Radio on a Chip* (PRoC) CYWUSB69 microcontroller with integrated 2.4GHz radio transceiver, as we illustrate in Figure 8.1 and Figure 8.2. Additionally, Cypress' WirelessUSB technology can be configured for point-to-point or multipoint-to-point contexts. You may be asking yourself, "what is new about this technology?" as the notion to marry wireless and USB has been around for some time.

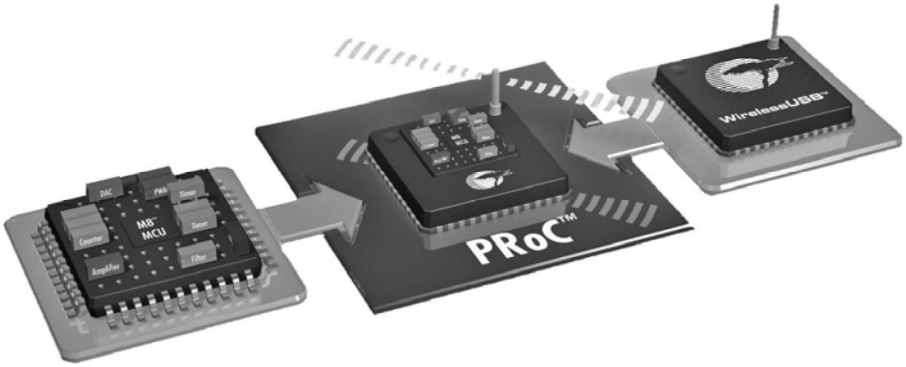


Figure 8.2
A conceptual representation of Cypress WirelessUSB solution with PRoC flash programmable microcontroller and integrated 2.4GHz radio transceiver.

For example, Bluetooth wireless technology was the first to boast the possibility of extending the USB ethos into a wireless medium; and then came along *Ultra-wideband* (UWB) purporting outrageous data rates of up to 1Gbps. You can read more about UWB in Chapter 15, *Ultra-Wideband: Introducing a New Short-Range Wireless Medium*. The curious among us would now ask: where is it? Indeed, where is the technology that was set to revolutionize and bring USB into the 21st century? God knows, is a possible answer; but let's forget the folly of the gossip and look at a much more realistic solution. More specifically, at a company that has chosen to move forward and bring a viable WirelessUSB solution to a market that covertly needs to see an evolutionary leap to bring the PC into the 21st century and, in doing so, complement an existing base of wireless technologies. But before we do that, we should look at the company's background and learn of what attributes that differentiate Cypress from other semiconductor companies.

Background

In comparison to our two proprietary solution providers in this section, the Cypress Semiconductor Corporation is a major contender in an industry that has seen a saturated mix of wireless technologies clawing at the same illusive trophy. With the clout and incomparable backing to other silicon providers, Cypress is a company to take extremely seriously. Cypress has already seen phenomenal success in the semiconductor industry and WirelessUSB surely is another notch in its overused headboard. It has a portfolio breadth expending a range of wired and wireless products, image sensors, timing and optical solutions, and so on. It is currently traded on the *New York Stock Exchange* (NYSE) and continues to be a formidable solution at the heart of any system.

The WirelessUSB Challenge

USB serves a plethora of peripheral devices, such as a keyboard, mouse, joystick, printer, external hard drive or CDROM, broadband modem, and so on. The challenges presented to WirelessUSB to outshine the facets of an existing and well-established technology are certainly daunting. In fact, WirelessUSB doesn't really have to do that much to stand out, as the basic premise itself is the removal of the cable, so from a consumer's perspective the same flexibility and simplicity inherently exists. Indeed, Cypress hasn't necessarily shunned away from such a daunting prospect, as it already provides USB chip solutions for USB v2.0 and USB *OnTheGo* (OTG) and surely melding a wireless semiconductor with USB silicon should be effortless. The *Human Interface Device* (HID) has been characterized as a piece of equipment that is connected to a PC. It enables a human to input data and takes many guises as we have already outlined. You may have passed by that frivolous reference: "melding" of technologies, but we will revisit this in some more detail in the following sections. Cypress seems to have a distinct advantage within the WirelessUSB domain, as the existing portfolio shows. As we will discuss in this chapter we will inevitably learn of exactly how Cypress' WirelessUSB semiconductor and its component base are architected, as well as understanding key factors that distinguish its radio technology from other competitors.

The RF composition

Cypress' WirelessUSB utilizes the overcrowded *Industrial, Scientific and Medical* (ISM) 2.4GHz band. What seems to differentiate the typical usage of the 2.4GHz band, in this instance, is the application of the DSSS, which has three operating modes, namely 64 chips/bit single channel; 32 chips/bit single channel and 32 chips/bit single channel *Dual Data Rate* (DDR). The first mode (64 chips/bit single channel) supports a single data stream operating at 15.625kbits/s where the advantages are the ability to tolerate noisy environments and enhancing data transmission over greater distances. In comparison the remaining two modes offer varying data stream rates. Within a DSSS-enabled system each data bit is transmitted as a *pseudo-noise* (PN) where each element of the PN-code is called a *chip*. If a DSSS-enabled device occupies an area which is susceptible to interference there is a greater likelihood of a transmitted PN-code to be received with some chips corrupted. The DSSS system will use a correlator to decode the incoming data payload where it determines if the number of errors is less than the correlator threshold. If the number of errors is less than this threshold, then the data is to be received correctly. In short, it is likely that the WirelessUSB system will successfully coexist and receive data without experiencing too many errors on the varying frequencies. In Figure 8.3 we illustrate how a WirelessUSB system determines quiet channels between other wireless technologies operating within the same ISM band. Although, introducing WirelessUSB in proximity with other technologies, such as WiFi or a cordless telephone may increase the probability of excessive interference. Additionally, the receiver and transmitter are a single conversion *low-Intermediate Frequency* (low-IF) solution that includes several integrated filters, which ultimately achieve high performance in the event of interference. The integrated *Voltage Controlled Oscillator* (VCO) and synthesizer offer the agility that enables the transmitter to cover all the channels in the ISM band. It appears that there are forty-nine spreading codes that have been selected for optimal performance, which are further supported across seventy-eight 1MHz channels, in turn, providing a theoretical spectral capacity of 3,822 channels. Evidently the

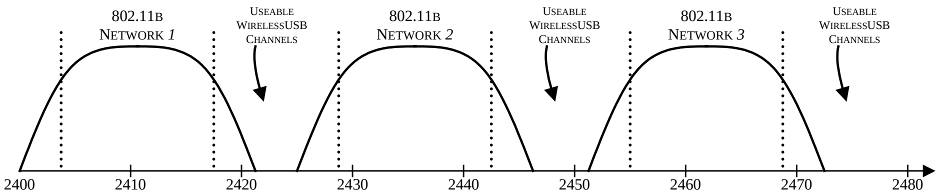


Figure 8.3 *In the presence of three 802.11b wireless networks, WirelessUSB sources useable quiet channels.*

2.4GHz band is also used by Bluetooth and WiFi (802.11b/g) and confidently you may be asking questions that are reminiscent of the Bluetooth vs. WiFi debate. Invariably, questions of coexistence come to mind, as we are already aware of the issues surrounding interference. You may be interested in referring to Chapter 4, *Can we Confidently Rely on Wireless Communication?* where we discuss coexistence and interoperation in some more detail.

Why do so many manufacturers choose to develop products with the ISM 2.4GHz band? There are of course other ISM bands available for use such as the 27MHz band, which is already used for an existing range of wireless keyboards and mice products. And, there are the 47/49MHz and 900MHz bands, which are also both used in various HIDs and many wireless stereo home products. The problem with these other bands is that the legislation allowing them to be used for HID-like applications differs from country to country. And, naturally developing silicon or creating a variant for each country will prove to be uneconomical, with an increased *Bill of Materials* (BoM), as well as proving to be problematic for manufacturing. In comparison the 2.4GHz band is available globally and with an increased uptake of the technology it has seen numerous countries adopt a more flexible approach in its regulation criteria.

The popularity of the 27MHz band has seen an increased wealth of HID applications flood the market. However, the 27MHz band has hindered the generic acceptance and development of HID products, as it has limited range and marred performance when compared with 2.4GHz. The 900MHz was also chosen to overcome the initial shortcomings of the 27MHz band, but this too has had its fair share of limitations. Most unnerving with the 900MHz technology is the deployment of wireless home speaker systems and the almost compulsory requirement of making any product wireless. As such, a 900MHz-enabled technology shouldn't necessarily reassure a consumer, but merely the consumer should reflect upon what other wireless technologies s/he is using in their home, as you might find that your cordless phone interoperates with your home/personal entertainment system which now seems to offer you a robust *Public Address* (PA) system. At the same time, the 2.4GHz band was a superior option, but its selection was inhibited by cost and developers were resorted to select inferior solutions (such as the 27MHz and 900MHz bands). Nevertheless, as the popularity of 2.4GHz increased, with nowadays an overcrowded range of products, so too has the price reflected its surge in popularity. The 2.4GHz band offers not only a negligible difference in cost, but offers, most importantly, improved reliability in performance. The essential ingredient with consumers accepting wireless products is ensuring reliability and cost. Certainly, if a consumer already has a wireless HID keyboard or mouse perhaps using the 27MHz or 900MHz bands and has not had a satisfactory user experience, then s/he is more than likely not going to choose another wireless product. More often the consumer will ultimately need a good reason for selecting a new 2.4GHz-enabled wireless keyboard, for example. Most significantly, consumers can be assured of low-latency, where there isn't a perceived delay in moving the mouse and the pointer doesn't necessarily correlate to your perceived location. Similarly, keyboard users can be assured that when a letter is typed it *will* appear on the screen and so on.

Crossing the bridge

We touched upon earlier in this chapter that the melding of two silicon technologies was required to bridge USB silicon to the WirelessUSB solution. It seems that some true words are spoken in jest and, indeed, this is exactly what occurs. A host PC for example, will not be aware of the WirelessUSB *bridge*, as the PC only recognizes the existing USB interface. As far as the PC is concerned it has attached a number of peripheral devices that directly interface with the USB mechanism, as we illustrate in Figure 8.4. In revisiting our initial ingredients for realizing WirelessUSB, it does appear to be a case of taking USB and a generous soupçon of wireless.

WirelessUSB for sensor networks

It seems that Cypress' vision isn't limited to HID-enabled devices; they extend their WirelessUSB portfolio to include sensor networks. In Figure 8.5 we illustrate a typical block structure of a WirelessUSB sensor application. The transition from enabling HID applications to enabling a sensor-like environment is not too difficult to conceive. Naturally, all the important considerations have been addressed, such as low cost, low power, security and so on, that we will touch upon in a moment. The sensor market for the home does seem to be saturated with various technologies; for example, in this book alone we discuss technologies from ZenSys and ZigBee, and we can be assured that there are a myriad of other technologies out there purporting similar advantages. You may want to refer to Chapter 7, *ZenSys: An Open Standard for Wireless*

Figure 8.4 *The host PC is not aware of the WirelessUSB bridge as the interface to the PC is the existing USB technology. In utilizing the WirelessUSB technology several devices can be connected to the host PC through the one wireless connection.*

Home Control, and Chapter 12, *ZigBee: Untethered and Unlicensed*, for further information about these technologies.

In the instance of *Developing Practical Wireless Applications*, manufacturers have a wealth of technologies to choose from. Naturally, you have a dichotomy in approach, such that in one hand you have the standardization philosophy while in the other,

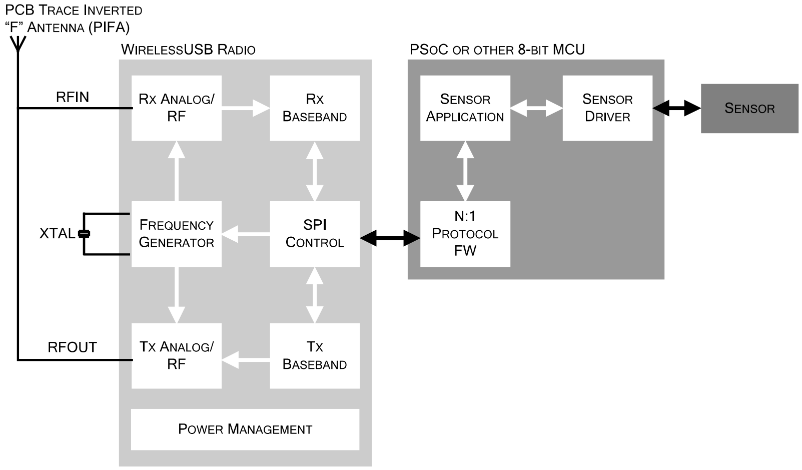


Figure 8.5 *A typical block structure of a WirelessUSB sensor application.*

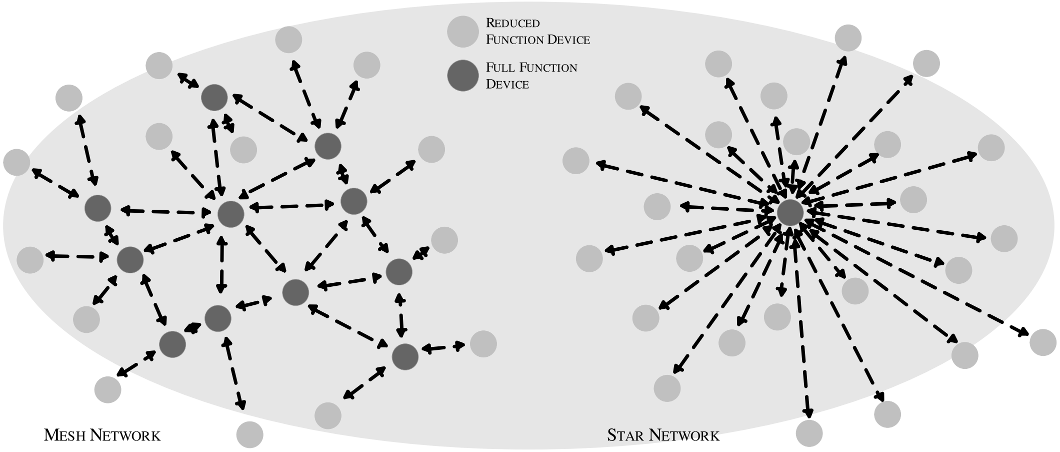


Figure 8.6 *In a similar vein to that of ZenSys and ZigBee, Cypress' WirelessUSB comfortably accommodates sensor technology offering identical networking topologies.*

a proprietary solution. There are a number of advantages in choosing Cypress' WirelessUSB solution as a sensor technology. With the ability to communicate over distances of fifty meters or so, there seems to be an increased probability of removing the need for a *repeater* device. A repeater device would be required to logistically extend a *nodes* range in a home networking topology, as we illustrate in Figure 8.6. Cypress' WirelessUSB silicon is offered in several flavors, notably various transmission ranges that suit different applications. For example, the WirelessUSB *LS* radio has a range of ten meters or so, which is better suited to the HID applications we already discussed. In comparison, the WirelessUSB *LR* radio is capable of transmitting over fifty meters simply relying on battery life alone; add an external power supply and it is capable of supporting a range of over 500 meters. Consumers are becoming increasingly aware of the need to have an extended battery life, as their wireless products, albeit cable-free, now rely on their own self-sufficient power supply. In the context of sensor technology some solutions require an increased duty cycle, implying that the node is communicating more regularly and thus consuming additional power. The duty cycle within some networking technologies, such as mesh and peer-to-peer, require higher duty cycles in order to maintain the integrity of the network. Conversely, WirelessUSB enjoys a comfortable sleeping duty and, as such, doesn't communicate as regularly as other network topologies.

In concluding this chapter we shall briefly consider one remaining aspect of our WirelessUSB solution and that is, security. Cypress recommends the public domain *Tiny Encryption Algorithm* (TEA) for use within any of its WirelessUSB products.

TEA is a fast and efficient cryptographic algorithm that utilizes a *Feistel* cipher where orthogonal operations are derived from *eXclusive-ORing* (XOR), *adding* and *shifting*. And, incidentally, TEA is very secure: at the time of writing there has been no known successful cryptanalysis of the algorithm (Simon Shepherd, Professor of Computational Mathematics, Director of the Cryptography and Computer Security Laboratory, Bradford University, England, 2006).

Conclusion

Cypress may indeed have a formidable portfolio and unimaginable authority in this industry that is second to none, but consumers are ultimately our judges and executioners, as we discussed in Chapter 1, *Making Sense of Wireless Technology*. The key to Cypress' success with WirelessUSB is to integrate their technology into the PC and its associated peripheral devices (the provision of WirelessUSB as a sensor technology can only boost Cypress' already diverse portfolio). If WirelessUSB is developed as an add-on to the PC, then the consumer, to be honest, already has a baffling choice of wireless wannabes. Cypress does indeed provide easy-to-use development kits for other companies to adopt its technology and for the manufacturers that create the peripheral devices – then this surely is a must. Using WirelessUSB within a PC is an inescapable evolutionary step for everyday consumers. Nonetheless, Cypress should push and align with PC manufacturers to ensure that their technology is at the wireless heart of every home and office PC.

Summary

- USB has been around for almost as long as the PC.
- The simplicity afforded by USB has perpetuated the notion of connectivity as a simple means of plugging one end into another.
- Many OSs have moved on to making life much simpler for the everyday consumer.
- The advent of wireless was expected to ease the transition from cables to a cable-free environment.
- To marry wireless with USB has to be genius.
- Who'd have thought that the combination of such simple ingredients to make WirelessUSB would have been so simple.
- Cypress Semiconductor have the right ingredients for WirelessUSB.

- Cypress offers a patent-pending, frequency-agile, DSSS solution affording a combination of low power, reliability and alleviating coexistence.
- Cypress' WirelessUSB offers a range of up to ten meters and fifty meters.
- USB serves a plethora of peripheral devices, such as a keyboard, mouse, joystick, printer, external hard drive or CDROM, broadband modem, and so on.
- The challenges presented to WirelessUSB to outshine the facets of an existing and well-established technology are certainly daunting.
- Cypress already provides USB chip solutions for USB v2.0 and USB OTG.
- Cypress' WirelessUSB utilizes the overcrowded ISM 2.4GHz band.
- What seems to differentiate the typical usage of the 2.4GHz band, in this instance, is the application of the DSSS.
- Within a DSSS-enabled system each data bit is transmitted as a PN where each element of the PN-code is called a chip.
- If a DSSS-enabled device occupies an area which is susceptible to interference there is a greater likelihood of a transmitted PN-code to be received with some chips corrupted.
- The DSSS system will use a correlator to decode the incoming data payload where it determines if the number of errors is less than the correlator threshold.
- If the number of errors is less than this threshold, then the data is to be received correctly.
- It is likely that the WirelessUSB system will successfully coexist and receive data without experiencing too many errors on the varying frequencies.
- Introducing WirelessUSB in proximity with other technologies, such as WiFi or a cordless telephone, may increase the probability of excessive interference.
- The receiver and transmitter of the WirelessUSB technology are a single conversion low-IF solution that includes several integrated filters, which achieve high performance in the event of interference.
- The integrated VCO and synthesizer offer the agility that enables the transmitter to cover all the channels in the ISM band.
- There are of course other ISM bands available for use such as the 27MHz 47/49MHz and 900MHz bands.
- These bands are already used in a variety of HID applications.
- The problem with these other bands is that the legislation allowing them to be used for HID applications differs from country to country.
- Developing silicon or creating a variant for each country will prove to be uneconomical, as well as proving to be problematic for manufacturing.

- The 2.4GHz band is available globally and with an increased uptake of the technology it has seen numerous countries adopt a more flexible approach in its regulation criteria.
- The 27MHz band has hindered the generic acceptance and development of HID products, as it has limited range and marred performance.
- The 900MHz was also chosen to overcome the initial shortcomings of the 27MHz band, but this too has had its fair share of limitations.
- The 2.4GHz band is a superior option and, most importantly, offers improved reliability in performance.
- The melding of two silicon technologies is required to bridge USB silicon to the WirelessUSB solution.
- A host PC will not be aware of the WirelessUSB bridge, as the PC only recognizes the existing USB interface.
- It seems that Cypress' vision isn't limited to HID-enabled devices; they extend their WirelessUSB portfolio to include sensor networks.
- The wireless sensor market for the home does seem to be saturated with various technologies.
- Cypress offers the ability to communicate over distances of fifty meters or so, in turn, removing the need for a repeater device.
- The WirelessUSB LS radio has a range of ten meters or so, which is better suited to the HID applications.
- The WirelessUSB LR radio is capable of transmitting over fifty meters.
- Cypress recommends the public domain TEA for use within any of its WirelessUSB products.
- TEA is a fast and efficient cryptographic algorithm that utilizes a Feistel cipher.
- Orthogonal operations are derived from XOR, adding and shifting.
- There is no known successful cryptanalysis of the algorithm.

9

Aura Communications Technology: Creating the Personal Bubble

Choosing an unknown path may lead you to places never discovered. Equally, the path you take may prove to be bumpy; once you've started it becomes difficult to turn back. However, it may also prove to be an exciting and thrilling opportunity to tread a path that has never been explored, like creating new footprints in the snow. Now merge these feelings with an overwhelming passion and unequivocal perseverance to complete your journey. It's inevitable that you will become infused with a sense of disbelieving triumph. With Aura Communications (www.auracomm.com) we are presented with a technology that ultimately has chosen an uncharted route to develop main stream technology and, in turn, create a whole new perspective on wireless connectivity. With a radio spectrum open to all, namely the *Industrial Scientific* and *Medical* (ISM) band 2.4GHz, 5GHz and so on, Aura chooses a lesser known magnetic induction technique with an operating frequency of 13.56MHz, which occupies the lower-end ISM band. Nevertheless, the technology has been with us for several decades and it is with Aura's ingenuity that its creators have chosen to apply the magnetic induction technique more practically (incidentally, we discuss in greater detail the application of *Near Field Communication* (NFC) and *Radio Frequency Identification* (RFID) in Chapter 14, *Near Field Communications: The Smart Choice for Enabling Connectivity*, where some comparisons can be made with the LibertyLink). In Aura's favor it has already submitted five successful US patents, along with multiple US and international applications that are filed and pending.

What we discuss in this chapter is a company that has chosen a new path, defied the norm and created a technology that unleashes unobtrusive proprietary wireless

Figure 9.1 *Aura Communications' LibertyLink (LL888) Integrated Circuit.*

communications. Its modest rationale is to deliver wireless stereo capability for the consumer electronics market. Additionally, we will ultimately discover what drives Aura to become a de facto standard where Bluetooth wireless technology seems an obvious choice for most manufacturers. We shall naturally examine the true character of Aura's *LibertyLink* (LL888) *Integrated Circuit* (IC), see Figure 9.1, and learn of the properties that uniquely set it apart from other more established methods of wireless connectivity. Likewise, we shall learn of its application potential that remains untouched by the already overpopulated radio spectrum. Confident of reaching large-scale consumer penetration, Aura Communications is a proponent of a technology that cohabits comfortably with other ISM-based wireless technologies.

Background

Aura Communications, with its headquarters in Massachusetts and offices in Asia, remains a privately held, venture backed company. It has already secured $31 million from investors such as Creative Technologies, Motorola Ventures, Duchossois Technology Partners, Entrepia Ventures and iSherpa Capital. It is a fabless semiconductor company that has developed the next generation of wireless freedom and portability with a sincere ambition to secure the technology as a de facto solution for streaming wireless voice and audio in the consumer and mobile arena. With established partnerships such as Creative (www.creative.com), Liquid Audio Asia (www.liquidaudioasia.com) and FreeLinc (www.freelinc.com), it is evident that Aura Communications has no desire to make a retreat from its uncharted path.

Near Field Magnetic Communication

In the majority of wireless communication systems a *Radio Frequency* (RF) wave is propagated through *free space*. The communication system supplies an *alternating current* (AC) to an antenna which, in turn, generates an *electromagnetic* field. In developing a wireless technology solution with an aim to penetrate mainstream consumerism you would naturally consider many RF propagation techniques along with your frequency of operation. This partnership can be likened to an arranged marriage: on one side of the partnership you have a radio, a tried and trusted piece of technology, which on occasions can be fickle. On the other side, you have a radio spectrum; you may not like it at first, but you eventually become accustomed to the unusual idiosyncrasies and the countless others who have already used it. Nonetheless, with time and patience you inevitably grow to like it and become complacent.

Near Field Magnetic Communication (or NFMC) uses a non-propagating, quasistatic magnetic field technique to achieve wireless connectivity between two devices. An RF plane wave flows through free space where a receiving antenna captures the alternating electromagnetic field. The RF propagation can extend tens, hundreds and even many thousands of meters. In contrast, NFMC does not depend upon receiving an electromagnetic field; instead a magnetic field is localized around the transmitting device. This technique translates to a low power solution that affords a predictable range and performance. In terms of performance, the LibertyLink supports a battery life of approximately fifteen hours based on a 260mAh rechargeable lithium battery. Furthermore, as there is negligible far field propagation of RF, the communication pathway between two devices becomes inherently secure.

The ability to transmit data is characterized in the time varying magnetic field, which is captured by the receiving device's *transducer* (a device that converts one form of energy into another). A negligible amount of RF propagation occurs at the carrier frequency (13.56MHz), but predominately the energy contained within the magnetic field uniquely defines magnetic communication and its data transfer properties.

Making bubbles

Additional characteristics can also be attributed to magnetic communication and, in particular the *roll-off* behavior as a function of distance. The power in an RF plane wave, in the far field, rolls-off as one over the distance from the origin squared, that is $1/r^2$. When we compare this to a quasistatic magnetic field we achieve a roll-off of $1/r^6$. In Figure 9.2 we illustrate a relative comparison of RF power and field strength (the E-Field), and magnetic field values (the B-Field).

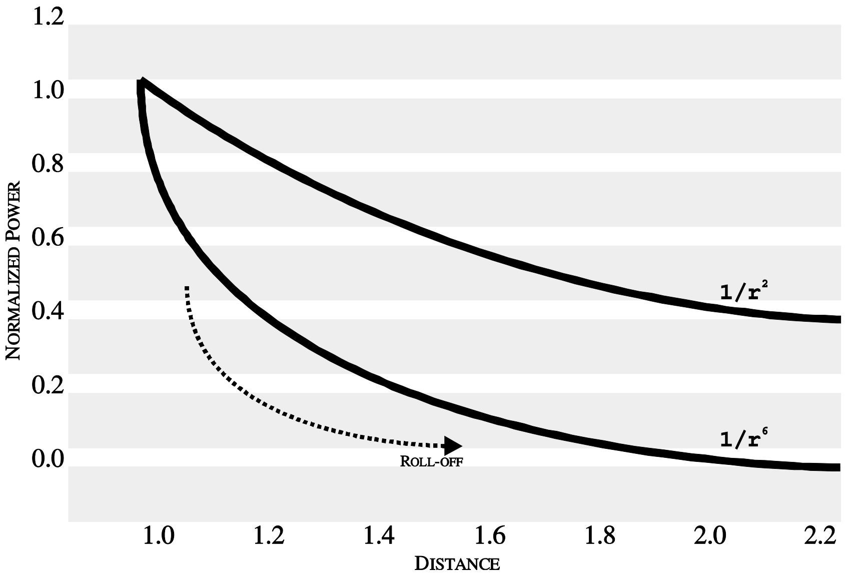


Figure 9.2 *A comparative representation of the roll-off behavior versus distance for a typical RF plane wave ($1/r^2$) and a quasistatic magnetic field ($1/r^6$).*

Initially, most of us would argue that a communication system based on strong *attenuation* (a decrease in power of a radio wave over distance) would have severe disadvantages. Naturally, any wireless communication system transmitting data over a greater distance would have to marry RF along with better attenuation properties. Nevertheless, for personal-area communication environments, as we discussed in Chapter 3, *Comparing Wide-area and Personal-area Communications*, it has some extraordinary benefits.

What is created through strong attenuation is a localized area of communication or put more simply, "bubbles," as we illustrate in Figure 9.3. In Figure 9.4 we illustrate a consumer who has an assortment of communication devices that interact wirelessly with each other. The consumer in this illustration may carry her products around in her pocket or backpack. This space around her is private and thus reinforces the personal nature of her consumables. You may recall our discussion regarding *BlueJacking* and *War-Chalking* from Chapter 4, *Can we Confidently Rely on Wireless Communication?*, where we highlighted covert capturing techniques of private and more often confidential information from devices such as *Personal Digital Assistants* (PDAs) and cellular phones. NFMC lends itself aptly in achieving a more secure environment.

Furthermore, a bubble will occupy a space of one to two meters (approximately three to six feet) as we illustrated earlier in Figure 9.3. This provides additional benefits, such as reuse of the frequency spectrum, since the roll-off and attenuation properties are highly predictable. It also remains largely unaffected by the presence of metal

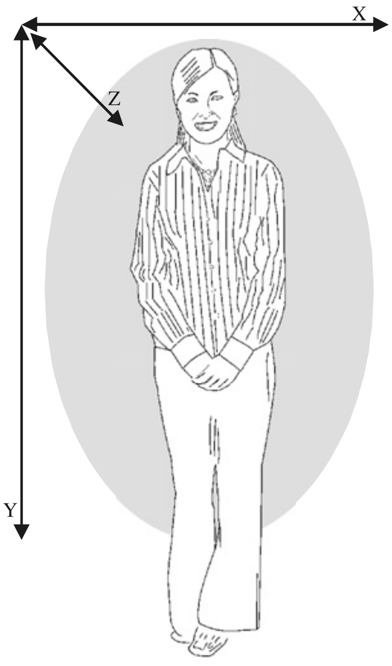


Figure 9.3 *The shaded area represents Aura's personal-area communication bubble.*

objects and other conductive materials, as well as individuals. In contrast, an RF plane wave, such as that utilized with Bluetooth wireless technology, is greatly affected by such objects and materials, and often the technology compensates by transmitting additional power to overcome the affects of signal loss; naturally, this has an impact on spectrum reuse and power consumption, in turn, affecting battery life. Moreover, an RF plane wave has greater propagation and, as such, wireless systems must be capable of sharing the allocated spectrum. For example, Bluetooth wireless technology uses

Figure 9.4 *A personal-area bubble comprises a collection of consumer electronic devices that typically communicate over a relatively short distance.*

Adaptive Frequency Hopping (AFH) to overcome issues of coexistence and a shared frequency spectrum; this generally leads to highly unpredictable RF signals in indoor and outdoor environments. Similarly, the consumer's body also affects the attenuation and again the technology has to compensate to overcome this unpredictability in radio wave behavior.

Propagation

We clearly understand the benefits and characteristics of near field magnetic communications, but implementing such a technology imparts its own challenges. One such consideration should be given to *polarization*, or the plane in which radio waves propagate. More specifically, in an RF-based system, a radio wave is formed with alternating orthogonal magnetic and electric fields (or *vector* fields). The field propagates in a direction perpendicular to the plane of the alternating fields. Polarization within a magnetic communication-based system, such as the LibertyLink, is highly dependent upon the transducer configuration. In a typical system, a ferrite rod, with a center of wound coil, would constitute a magnetic field source, see Figure 9.5. The properties of this type of antenna can be likened to a *dipole* (a dense force of magnetic energy).

In such a system, transmitting and receiving antennas have to be positioned to achieve the greatest *coupling* (at a given separation). In an ideal context two rods (transmit and receive) placed in a coplanar orientation, see Figure 9.6, would achieve maximum coupling. In comparison, if we place the receiving rod in an orthogonal orientation, reduced or no coupling occurs, see Figure 9.7. The consumer of a magnetic

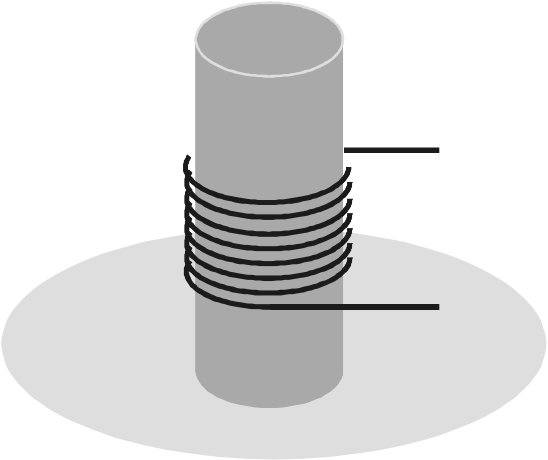


Figure 9.5
A ferrite rod with a center of wound coil provides the magnetic effect of a classic dipole.

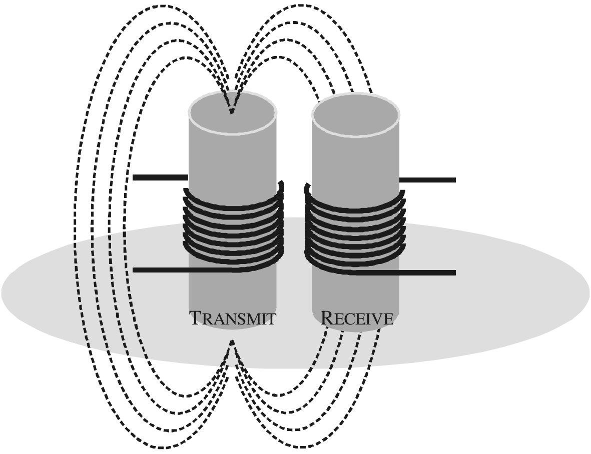


Figure 9.6
In a coplanar orientation coupling is highly effective between transmitting and receiving ferrite antennas.

communication system can be seen as a random entity offering great unpredictability in terms of how they would use and position a product. For example, a consumer may have an audio player in her pocket whilst wearing a stereo headset. She may be jogging or walking around in a shopping mall, so we can assume that the headset is moving around as she moves her head, looking at where she's running or perhaps at the various goods within shop windows.

To ease this unpredictability aspect and to ensure successful communication in any orientation, polarization diversity can be used to achieve greater coupling. In a stereo headset we can implement three receiving antennas in such a manner that signals are captured in all three orthogonal dimensions, see Figure 9.8.

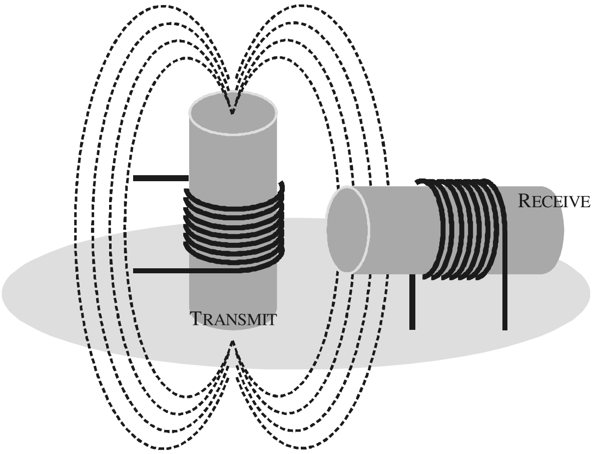


Figure 9.7
In an orthogonal orientation coupling is greatly reduced between transmitting and receiving ferrite antennas.

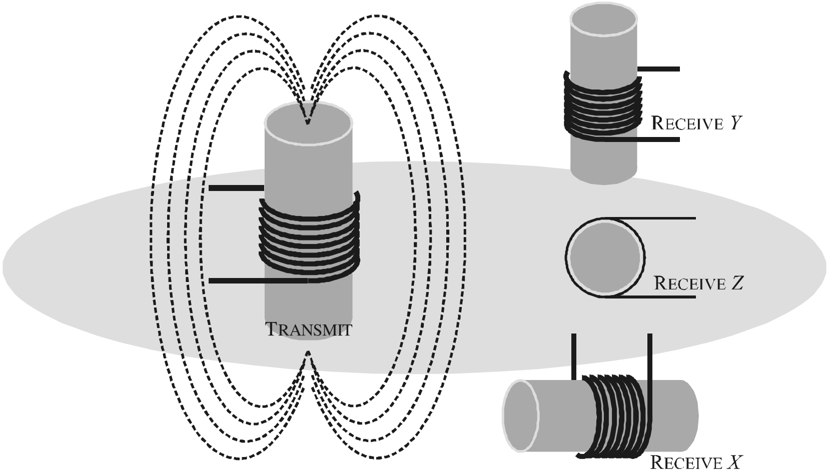


Figure 9.8 *Polarization diversity can be employed in a stereo headset to help reduce the unpredictability of a consumer; all three dimensional spaces can be captured (X, Y, Z).*

Initially, you may be contemplating that three antennas would, in turn, lead to larger headsets. A Bluetooth wireless antenna comfortably occupies the *Printed Circuit Board* (PCB) space, at most 15mm × 3mm, (0.6in × 0.12in), where the height is negligible. In contrast, the cubic space of the polarization diversity antennas occupies no more than 750mm^3 (less than 0.05 cubic inches). Naturally, this leads to more appealing consumer wearables.

Coexistence and interference

In our previous sections we have eluded issues surrounding the specific aspects of how NFMC overcomes the limitations imposed by other wireless technologies. We are aware that Bluetooth, ZigBee and WiFi (namely, 802.11b/g) occupies the already crowded spectrum space (2.4GHz) and how they might overcome such restrictions. We also discussed the impact upon boosting transmission to overcome these issues, but this has degrading affects on power consumption and increased the complexity of radio transmission and reception schemes. NFMC avoids most of these issues due to the localized magnetic energy. You may recall that we discussed the highly predictable roll-off and attenuation behavior leading to a bubble effect. This localization assures us security and reusable spectrum. Nevertheless, it seems that NFMC is not completely impervious to interference.

You may also recall that NFMC technology has been around for several years, being applied to other applications, namely RFID; this technology is discussed in more detail in a later chapter. In essence, RFID uses the same carrier frequency as

NFMC (13.56MHz). The premise of RFID is very similar to that of NFMC. It too creates a small bubble in which it communicates, allowing personal communication between *tags* and *transponders*, both of which contain antennas. For example, some metro (underground or tube) systems utilize this particular technology enabling commuters to move quickly through entry and exit points. Commuters simply pass a tag (credit card sized) across a reader (transponder) providing them access to or exit from the metro service. Similarly, some freeways (or motorways) have tolls which require a payment; commuters will have access to a dedicated lane with an electronic toll system enabling them to continue their journey more quickly.

RFID systems also rely on a bubble type communication environment and, as such, any NFMC-enabled equipment entering the same bubble and creating a communication overlap will undoubtedly cause some level of interference with other devices. Once the communication bubbles separate both systems resume normal operation due to the tolerable roll-off and attenuation schemes; a typical RFID system has a bubble only a few centimeters (inches) in radius.

Quality of service

Aura Communication wishes to achieve high-end market penetration with a solution that delivers audio and voice streaming. Such systems depend upon a guaranteed radio transmission and reception providing good *Quality of Service* (QoS). Bluetooth wireless technology seems an obvious choice, but (at the time of writing) some QoS issues are still being resolved, namely issues with the overcrowded spectrum. Many consumers within the US and Europe have complained of intermittent interoperability as there are quite a number of proprietary solutions that are already using the 2.4GHz spectrum; more about Bluetooth later in Chapter 11, *Bluetooth: A Cable Replacement Technology*. Bluetooth wireless technology is undoubtedly a predominant member in the cellular and headset community, but eventually it will want to dominate as the solution for a wireless stereo headset.

The LibertyLink offers a data rate of 410Kbps, whereas most voice applications only require 64Kbps. Since we are transmitting CD-like quality music, the LibertyLink uses a 4:1 compression ratio for its *Adaptive Differential Pulse Code Modulation* (ADPCM) and requires 384Kbps. A 384Kbps data obligation seems somewhat excessive, as most MP3 players only require around 128Kbps. However, this scope entertains a number of uncertainties. First, the *Bit Error Rate* (BER) of the ADPCM encoding scheme is tolerant to 10^{-5} enduring a small number of errors. Nevertheless, any drop-out (clicks, pops and so on) with music is likely to be unacceptable to any consumer. The higher bandwidth affords tolerances to interference, thereby always assuring the consumer of good QoS.

Conclusion

Aura Communications offers a solution that will provide good QoS in an already overpopulated wireless world. Its solution is power and cost effective friendly, enabling manufacturers to deploy products in the market – now! Ultimately, what drives effective product development is cost and Aura unashamedly meets this expectation.

One final thought: with increasing popularity with the NFC Forum and the eagerness to deploy similarly enabled technologies within the wireless community, Aura Communications will inevitably have to devise better schemes to overcome a new generation of personal-area environments. Simply put, being ahead in the market and being prepared for the inescapable will assure a true and lasting future in such an unpredictable wireless world.

Summary

- With Aura Communications we are presented with a technology that ultimately has chosen an uncharted route to develop main stream technology.
- Aura has created a whole new perspective on wireless connectivity.
- Aura has chosen a lesser known magnetic induction technique with an operating frequency of 13.56MHz.
- The frequency occupies the lower-end ISM band.
- Aura's rationale is to deliver wireless stereo capability for the consumer electronics market.
- Aura Communications is a proponent of a new wireless technology.
- An RF wave is propagated through free space; such communication systems supply a current to an antenna. In turn, this transmits an electromagnetic field.
- This arrangement can be likened to an arranged marriage.
- NFMC uses a non-propagating, quasistatic magnetic field technique to achieve wireless connectivity between two devices.
- RF propagation can extend tens, hundreds and even thousands of meters.
- NFMC does not depend upon receiving an electromagnetic field, instead a magnetic field is localized around the transmitting device.
- This technique translates to a low power solution that affords a predictable range and performance.
- The LibertyLink supports a battery life of approximately fifteen hours based upon a 260mAh rechargeable lithium battery.

- NFMC is inherently secure.
- The ability to transmit data is characterized in the time varying magnetic field, which is captured by the receiving device's transducer.
- A negligible amount of RF propagation occurs at the carrier frequency (13.56MHz).
- In a quasistatic magnetic field we achieve a roll-off of $1/r^6$.
- Most of us would argue that a communication system based on strong attenuation would have severe disadvantages.
- What is created through a strong attenuation methodology is a small sphere of communication or, put more simply, "bubbles."
- A bubble will occupy a space of one to three meters (approximately three to nine feet).
- Benefits such as reuse of the frequency spectrum can be enjoyed.
- NFMC's roll-off and attenuation properties are highly predictable.
- It also remains unattenuated by the presence of metal objects and other conductive materials, as well as individuals.
- An RF plane wave, such as Bluetooth wireless technology, is greatly affected by such objects and materials.
- Implementing the LibertyLink imparts its own challenges.
- Polarization within a magnetic communication-based system is highly dependent upon the transducer.
- In such a system, transmitting and receiving antennas have to be positioned to achieve the greatest coupling.
- In an ideal context two rods placed in a colinear orientation would achieve maximum coupling.
- In comparison, a receiving rod in an orthogonal orientation will reduce coupling.
- The consumer has great unpredictability in terms of how they would use and position a product.
- Antenna diversity can be used to achieve greater coupling in most consumer contexts, in turn, easing consumer unpredictability.
- In a stereo headset we can implement three receiving antennas in such a manner that all three dimensions can be captured.
- Implementing three antennas does not consume a lot of space, leading to more appealing consumer wearables.
- It seems that NFMC is not completely impervious to interference.
- RFID uses the same carrier frequency as NFMC (13.56MHz).

- The premise of RFID is very similar to that of NFMC.
- It too creates a small bubble in which it communicates, allowing personal communication between tags and transponders.
- Creating a communication overlap with NFMC and RFID will cause interference with the devices.
- Once the communication bubbles separate both systems resume normal operation due to the tolerable roll-off and attenuation schemes.
- Audio and voice streaming depend upon a guaranteed radio transmission and reception providing good QoS.
- The LibertyLink offers a data rate of 410Kbps, where most voice applications only require 64Kbps.
- The LibertyLink uses a 4:1 compression ratio for its ADPCM, which only requires 384Kbps.
- 384Kbps data throughput seems excessive, as most MP3 players only require around 128Kbps.
- This throughput enables a more robust link for audio applications.
- The *Bit Error Rate* (BER) of the ADPCM encoding scheme is tolerant to 10^{-5} tolerating a small number of errors.
- Any music drop-out is likely to be unacceptable to any consumer.
- The excessive bandwidth affords tolerances in respect of interference always assuring the consumer of good QoS.
- Aura Communications offers a solution that will provide good QoS.
- Its solution is power and cost effective friendly, enabling manufacturers to deploy products in the market – now.
- With increasing popularity of the NFC Forum Aura Communication will have to devise improved schemes to overcome a new generation of personal-area environments.

Part Three

A Standards Approach to Developing Wireless Applications

This page intentionally left blank

10

An Introduction to the Notion of Standards-based Wireless Application Development

Perhaps our introduction in Chapter 6, *An Introduction to the Notion of Proprietary-based Wireless Application Development*, was a little unforgiving? Non-profit standardization organizations each with an objective to steer and drive the future of their respective technologies have their purpose and the best interest of manufacturers and consumers alike. Admittedly, there are countless acronyms, *three letter abbreviations* (TLAs), compliance and interoperability specifications, which *may* lead to confusion, and perhaps, our reference to "boredom" was a little zealous. The standardization process is to assure the developer community that a product from one manufacturer will interoperate with another. With regular attendance at (un)plugfests we are additionally assured that we will achieve successful interoperation. This process also enables developers to smooth out any ambiguities with the specification and allow them to test the product with other similarly enabled products from various manufacturers.

We can still envisage our four year roadmap with a technology that has been thoroughly tested by a testing house, and of course we can choose to use the associated logo and other branding. Our eager desire to deploy the latest wireless-enabled products remains deep-seated, but manufacturers can be assured of a technology that will be globally accepted by an international community. There are numerous companies that will gladly take on the burden of the constraints and expectations to abide by a myriad of rules and regulations which undoubtedly for any organization is a daunting prospect. A standardized technology affords the consumer flexibility in product choice and assures them of successful interoperability.

Case Studies

This chapter introduces to you some commonplace and new personal-area technologies that have shaped or will shape the way in which we work and live. In particular Table 10.1 identifies just five of those technologies.

Table 10.1 *A selection of standardized technologies that afford consumers of interoperability and product choice*

Standard	Chapter	Description
Bluetooth	Chapter 11	A Cable Replacement Technology
ZigBee	Chapter 12	Untethered and Unlicensed
WiFi	Chapter 13	Enabling True Ubiquitous Connectivity
NFC	Chapter 14	The Smart Choice for Enabling Connectivity
UWB	Chapter 15	A New Short-Range Wireless Medium

11

Bluetooth: A Cable Replacement Technology

The thought of dipping into the various Bluetooth-specific specifications is something which shouldn't be done lightheartedly. An engineer suitably equipped with a jug of coffee and other caffeine-based products should only then, but not necessarily advisably, embark upon the thousand or so pages. The page count doesn't stop there either; with the new release of the Specification of the Bluetooth System and the many adopted profiles, we will surely see an emerging wealth of detailed information ready to be ingested by the most fearless. The release of the Specification of the Bluetooth System: Core v2.0, plus *Enhanced Data Rate* (EDR) offers backward compatibility with v1.2 and the ability to support a host of other profile enhancements. And, of course, we already have a series of adopted profiles that have been prepared and incorporated into a formal release of the *Specification of the Bluetooth System: Profiles*. With the recent marriage of Bluetooth and *Ultra-wideband* (UWB) we may even witness a new evolution to the specification suite; perhaps we can hear the pounding keys of a keyboard thrashing out the *Specification of the Bluetooth System: Core v3.0* with an accompanied wealth of new profiles complementing the array of new Bluetooth/UWB-enabled applications. This continued growth is evidence of a technology that has taken up permanent residence in communication-enabled products, albeit those predominantly targeted towards the cellular market (phone and headset). The plethora of Bluetooth-orientated product flyers occupies much of the window space in our local high streets, tempting us to abandon our cables for simpler useability. With its growth predicted to overtake that of WiFi, Bluetooth technology demonstrates that it has an undying ambition to govern our everyday use of technology (some reports have already witnessed the growth of Bluetooth exceeding that of WiFi; it really comes down to whom you believe, as Bluetooth has only captured a niche market). In Chapter 13, *WiFi: Enabling True Ubiquitous Connectivity*, we adopt a more realistic perspective about the success and enormous market penetration of WiFi where we have seen an unparalleled acceptance of the technology covering a wide spectrum of application areas. Bluetooth wireless technology's success is evident in the cellular market. Indeed, this is further heightened in the United Kingdom, the United States and, similarly, other European countries where local and/or national Governments have made it an illegal offence to operate a cellular phone within a vehicle. Drivers, in turn, are only allowed to operate hands-free devices. Those caught holding a cellular phone within their vehicle will receive an on-the-spot fine and will automatically accrue three penalty points on their driving license (this refers to UK-specific law and penalties). As such, it has increased the popularity of the automotive Bluetooth working group and technologies surrounding the potential deployment, which detail scenarios that conform to the now frowned upon use of a cellular phone within a moving vehicle. Nowadays, perusing the vehicle manufacturers' brochures, even for some of the basic ranges of vehicles, an option for Bluetooth wireless technology hands-free capability is usually available at an additional cost. Naturally, at the far end of the vehicle spectrum the technology has become an integral component of the car or, at least is being introduced as a no-cost option, offering wireless connectivity as standard; a handful of car manufacturers have already ventured into this area, which is increasingly becoming prevalent.

The momentum of Bluetooth wireless technology is accelerating at a phenomenal rate within applications surrounding the cellular and audio market and, as such, has become the de facto short-range cable replacement standard. In the UK, Europe and increasingly the US, many consumers have chosen to interoperate their cellular phone with a Bluetooth-enabled headset, plainly supporting the new hands-free ethos. Similarly, with an increase in popularity of Apple's iPod generation of products, a somewhat natural evolution to the headset is to support wireless stereo functionality affording the freedom of cable-free use. You may recall in Chapter 9, *Aura Communications Technology: Creating the Personal Bubble*, we offered an alternative wireless solution for stereo headset operation based upon *Near Field Communications* (NFC). For those who can remember a day where so many critics were eager to place the nail into the Bluetooth coffin in its very early stages, we can now be assured of a technology reaching a level of maturity where vehicle, consumer electronic and cellular manufacturers (and hopefully the wider market population) can reassuringly consider it a viable wireless solution.

Bluetooth vs. Infrared

Undeniably, Bluetooth technology has its application-base firmly founded in Infrared. Even today, manufacturers have not abandoned this tried and trusted technology for the more omnipresent wireless equivalent. Take a closer look at your cellular phone and your notebook computer: *Infrared-enabled?* Again, take a closer look at your cellular phone and your notebook computer: Bluetooth- or WiFi-enabled? If you place two Infrared-enabled notebooks unassumingly beside each other you will become bemused as you begin to hear "whooshing" and "whirring" sounds along with an impromptu notification on your Windows taskbar informing you that you can now connect to your colleague's computer and transfer files. Similarly, placing your Infrared-enabled cellular phone alongside your computer would unassumingly instigate communication whilst in line-of-sight. This ability and sheer simplicity conveys a degree of confidence that has been unmatched by any other wireless technology to date (with the undeniable exception of the cellular market). A clear notification of intent to transfer files or any other information is visibly made clear to the user and, moreover, the impromptu notification allows the user to review any potential transactions. In Chapter 14, we discuss a similar notion of enabling communication between two devices.

But, does line-of-sight really matter? No. However, the founding premise of Bluetooth is that you no longer need to point at a device to make it do something. Bluetooth wireless technology has a lot to live up to: as we have already discussed and highlighted there is a certain element of success within the cellular industry. Moreover, Bluetooth now needs to encompass a wider market and maintain the offer of simplicity for it to succeed.

The Odd Couple: Bluetooth and Ultra-Wideband

But what is to be made of the newly formed alliance between Bluetooth wireless technology and UWB? Perhaps it's a case of "keep your friends close, but keep your enemies closer?" It is clearly evident that UWB offers higher data rates and establishes a more reliable data connection due to its multipath and wide bandwidth techniques (we discuss UWB in Chapter 15, *Ultra-Wideband: Introducing a New Short-Range Wireless Medium*). In many presentations of the UWB technology many have argued that Bluetooth and UWB are competitors. Similarly, on these occasions we may have become privy to numerous use cases illustrating how it would be possible for UWB to succeed where Bluetooth fails; some reports even dare to suggest that Bluetooth is dead. It really is too dark out there to see who is holding the hammer in a final attempt to drive in that last nail!

Nevertheless, it seems that, with a degree of predictability, following various announcements made by the Bluetooth *Special Interest Group* (SIG) and press agencies, industry commentators have unconditionally welcomed the extensible possibilities that UWB offers Bluetooth. With such amusement and chess-like frivolity you may witness key players that make-up the various standards bodies maneuvering themselves to other significant areas within a new organization like pawns in a political game; whilst they individually strive for organizational dominance and forsake a technology that they may have initially supported for a number of years. It seems as though it's a case of abandon ship and seek sanction and forgiveness in a new, albeit immature standards body that has yet to leave its mooring. Alas, it seems as though mortgages have to be paid and the bigger picture is forgotten. It is painfully clear that without such support from the wider industry Bluetooth would have surely suffered disbandment along with HomeRF. It is envisaged that UWB will be architected within the Bluetooth specification, in turn, enabling the much sought after higher data rates and the ability to penetrate popular audio/video types of applications. Furthermore, it has to be said that secretly Bluetooth has also been viewed by many in the industry as a technology struggling to penetrate key products within the consumer electronics market – although it has succeeded within the cellular market in many countries already. What is more evident is the poor uptake of Bluetooth in mainstream consumer electronics within the US and to a greater extent in the UK and Europe. This is largely rumored to be poor interoperation and coexistence related issues, due to a large number of proprietary-based wireless technologies already utilizing the 2.4GHz spectrum. With an incredible foresight, the Bluetooth SIG have refused to become stagnant in a market that demands change and expects improved functionality. In a continuous barrage of criticism, the SIG have been pushed into introducing modifications that have afforded it efficient discovery and pairing procedures, as well as modifying the most critical aspect: coexistence. In introducing an *Adaptive Frequency Hopping* (AFH) scheme Bluetooth provides a more harmonious coexistence with the large consumer base of proprietary and standardized wireless technologies.

Bluetooth over UWB

You may recall in Chapter 8, *Cypress Semiconductor: Introducing WirelessUSB*, we discussed the rich number of possibilities that *WirelessUSB* (WUSB) offered in terms of the standard PC and its associated number of peripheral devices. The marriage of Bluetooth and UWB can now realistically push a new generation of technology that will serve the WUSB dream much more satisfactorily, as the potential bandwidth seems to exceed that of existing USB-enabled products. When you compare Bluetooth's EDR offering data rates of up to 3Mbps and compare that with UWB's offering of up to a theoretical 1Gbps you may begin to understand the range of possibilities. It seems that UWB is riding Bluetooth's already established, albeit muted, market acceptance and through a back door we will undoubtedly witness UWB becoming the basis of most Bluetooth audio/video solutions. It is clear that this subtle approach will help avoid the thrusting of yet another new wireless product into the consumer's already crowded top drawer of USB- and PCMCIA-enabled devices.

WiMedia Me

The combination of UWB and Bluetooth technologies has manifested itself into a categorization known as WiMedia. Although, it seems that a full and final definition of what WiMedia is remains somewhat elusive; if you Google the definition you are presented with a myriad of choices which will ultimately leave you unsatisfied. Many articles refer to several personal-area wireless technologies arguing that each uniquely affords its own make-up of what WiMedia can do. However, if you refer to the WiMedia Alliance's website (www.wimedia.org) they seem to portray an image of unison between UWB and Bluetooth, supporting a genre of multimedia-centric applications for the consumer electronics industry. Ironically, it has taken the consumer a good number of years to understand what Bluetooth supports (Millward Brown) and now they have to ingest yet another wireless technology. It is clear that the collective spectrum offered by UWB and Bluetooth will be seen as WUSB and should afford a more harmonious introduction to the consumer, as it isn't a million miles away from USB and hey, you just don't need to use the cables!

In this chapter we consider the various building blocks required to create successful Bluetooth-enabled applications and also provide specific details of the protocol stack, alongside the diverse range of profiles that accompany the Bluetooth core specification. The range of profiles is pivotal in realizing a specific application, as it ultimately defines how that application should manifest itself to the user and how the user might interact with it. These significant components are first and foremost integral in developing Bluetooth-enabled wireless applications. However, we will first introduce the founding application-base that apparently led the way to overcoming Infrared's shortcomings. We shall also touch upon the origin of Bluetooth's inception. This will not be a tedious parody of "it was King Harald" and incessant references to Denmark (yawn), but will merely draw your attention to significant changes to the structure of the SIG (you know, those chess pieces). Furthermore, we will also discuss the radio architecture, as this uniquely sets apart the technology from other similar 2.4GHz-enabled wireless technologies, with its new AFH scheme proclaiming that it ensures much more of an amicable coexistence with technologies that already utilize the crowded spectrum.

The Original Bluetooth

Looking back at its inception, Ericsson was the first to conceive Bluetooth, which evolved from its *Multi Communicator Link* (or MC-Link) technology. Ericsson initially proposed a headset solution, but ventured into the possibility of interoperating with other devices, such as notebooks and other communication-based devices. Undoubtedly, this has now led to the emergence of numerous Bluetooth-enabled products that are currently available today. Furthermore, the door has opened to what has now become known as *Personal Area Networking* (PAN). Incidentally, you may recall from Chapter 3, *Comparing Wide-area and Personal-area Communications*, where we touched upon *personal-area* vs. *wide-area* technologies. The ability for your own personal devices to interoperate with each other without the need for cumbersome cables has led the way to create simpler ease of use scenarios for a whole range of users and consumers alike. To begin to undertake this global vision, Ericsson spun off a new company, *Ericsson Technology Licensing*, and this is where we begin to observe significant changes within the core and founding structure of the SIG. Ericsson Technology Licensing withdrew its interest from core Bluetooth development, causing serious cracks within the general Bluetooth community. Ericsson claims to be a continued proponent and key driver for the future of Bluetooth wireless technology alongside its promoter companies. Presumably you recall that Ericsson elected to make the technology an open global standard, in turn, allowing other manufacturers to share the responsibility of defining the technology and to increase its wider adoption? A consortium of promoter companies to include, Agere Systems, Ericsson Licensing Technology, IBM, Intel, Microsoft, Motorola, Nokia and Toshiba form the non-profit association that is the Bluetooth SIG, in addition to the large number of Associate and Adopter companies. You may have noticed within the series of promoters companies that 3Com has been omitted. 3Com was a key member within the SIG until it relinquished its position as promoter; at the time of writing the SIG have yet to replace the void left by 3Com's departure. You may now begin to understand that it is with these significant cavities (3Com and Ericsson Technology Licensing) that key figures within the SIG felt that the ship needed abandoning.

The Radio Architecture

Bluetooth, like 802.11b, ZigBee and a host of other proprietary wireless solutions, occupy the crowded 2.4GHz *Industrial*, *Scientific* and *Medical* (ISM) band with an operating range of 2400 to 2483.5MHz. Due to the unlicensed nature of the spectrum, manufacturers are able to utilize this band for any purpose and, as such, a range of products are already available on the market utilizing this radio frequency. The radio

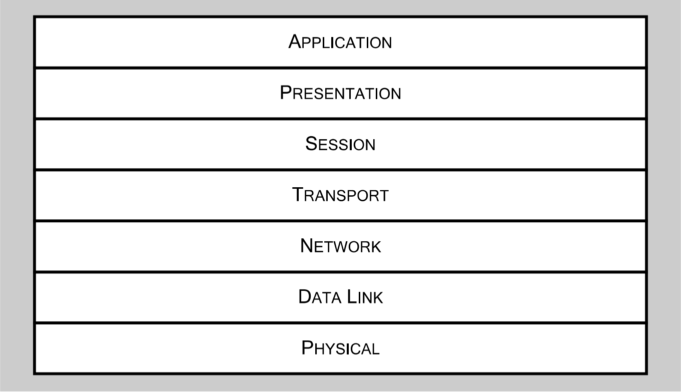


Figure 11.1 *The OSI model which, to a large extent, remains common to all wireless protocol stacks.*

along with its antenna forms part of the hardware that transmits and receives radio waves. The *Link Controller* (LC) interfaces with this hardware (more about the LC layer later on in this chapter) to facilitate communication to and from the radio. The LC layer can be likened to the *physical* (PHY) layer as compared with the *Open Systems Interconnect* (OSI) architecture model, see Figure 11.1. Despite occupying an overcrowded spectrum with a plethora of similarly unregulated wireless-enabled products, Bluetooth utilizes a series of short data packets and a *Time Division Duplex* (TDD) scheme to enable bi-directional communication. In addition to this, an adaptive frequency hopping scheme is used to overcome issues of coexistence and interference and a number of power classes are also supported enabling various operating power consumption schemes that all aim to provide a low-power communications medium. Furthermore, Bluetooth operates two modulation schemes, namely *Basic Rate* and EDR, the latter rate is optional, but both utilize the TDD scheme to support full-duplex communication. The Basic Rate scheme operates the *Gaussian Frequency Shift Keying* (GFSK) modulation scheme compared with EDR which uses the *Phase Shift Keying* (PSK) scheme (more about these schemes in the following section).

The frequency hopping scheme

The concept of *frequency hopping* has been with us since World War II. Primarily, the scheme was used to overcome issues surrounding security and reliability; moreover, it reduces the likelihood of the communications pathway being blocked, perhaps due to an abundance of devices already utilizing the 2.4GHz band or a deliberate attempt to do so. A retransmission scheme is used to help alleviate lost packets or packet collision with other devices in proximity, in turn, providing a more reliable transport service.

When a lost data packet occurs, the packet will be retransmitted on a different channel according to a pseudo-random sequence within the radio system; with seventy-nine channels available data loss is kept to a minimum. Initially, regulations within France imposed a limited number of operating channels to twenty-three. However, due to an initiative conducted by the Bluetooth SIG, frequency harmonization has now been achieved, where France utilizes the full seventy-nine operating channels. With an operating band of 83.5MHz (2400MHz to 2483.5MHz), spaced at 1MHz intervals and accompanied with a lower guard band of 2MHz and an upper guard band of 3.5MHz a frequency hop channel can be calculated using, $f = 2402 + k$ MHz, where k is the channel number, numbered between 0 to 78 (a lower and upper guard band is used to overcome any out-of-band regulations for a particular country). Allowing the radio to retransmit the data packet on a different channel will undoubtedly increase the probability of the packet being transmitted successfully. This pseudo-random sequence also makes it difficult for other devices within radio range to eavesdrop on the wireless communications link. Typically, devices have to be trusted parties to take part in any wireless conversation. You may recall from our discussion in Chapter 4, *Can we Confidently Rely on Wireless Communication?* where we touched upon the issue of creating trusted connections between Bluetooth-enabled devices by exchanging *passkeys*. A passkey is similar to a *Personal Identification Number* (PIN), which is shared between two or more users (or devices) of a Bluetooth PAN. When exchanging passkeys, Bluetooth-enabled devices become *paired*, where an *initialization key* is generated, allowing Bluetooth authentication to take place. Bluetooth authentication occurs when two or more devices share a common link key or initialization key, in turn, generated by the passkey. This procedure is based upon a challenge-response scheme. Devices that have been authenticated can then choose to use an encryption procedure, which will hinder other devices from overhearing the subsequent conversation. The pairing and encryption procedures are optional, but are certainly recommended in light of our earlier (Chapter 4) discussion surrounding *BlueJacking*.

With an expectation for Bluetooth technology to operate in both indoor and outdoor environments, several radio and system parameters are used to overcome the potential noise and interference, which should naturally be expected. The specification defines a raw *Bit Error Rate* (BER) of 0.1% and a receiver sensitivity of −70dBm. Although, in practice most Bluetooth radio manufacturers increase their sensitivities by 10dBm to ensure greater reliability and distances, above the prescribed recommendations.

Adaptive frequency hopping

You may recall in Chapter 4, *Can we Confidently Rely on Wireless Communication?* we discussed issues surrounding coexistence with other 2.4GHz-enabled products.

AFH is a scheme that was introduced by the SIG to reduce interference with a range of proprietary technologies that already use the 2.4GHz radio spectrum. Both 802.11b- and 802.11g-enabled products utilize the 2.4GHz radio spectrum and the market penetration of this technology is somewhat widespread. The existing frequency hopping scheme hops at a rate of 1,600 times per second where the scheme utilizes all 79 channels available within the 2.4GHz band. New generations of Bluetooth products will use the AFH to avoid conflicts within the available channel range. In an environment where there are many 2.4GHz wireless products, there is a greater probability that a collision will occur on a particular channel and, as such, data may be lost. AFH affords Bluetooth a more intelligent approach to its frequency hopping scheme, as it adapts to the environment in which it finds itself. If there is a consistent problem with a particular channel, then AFH will exclude this channel from the scheme. Interestingly, in a heavily populated environment, it is conceivable that the number of available channels would reduce considerably; however, the specification does dictate that the minimum number of channels readily available should be around twenty. Although the scheme helps reduce the likelihood of problems associated with coexistence it is still not completely dependable.

Basic rate and enhanced data rate

A maximum data bandwidth of 1Mbps is achieved through the Basic Rate GFSK modulation scheme, utilizing a *bandwidth-bit time* (BT) product of 0.5 and a modulation index of between 0.28 and 0.35. Uniquely, the GFSK modulation scheme denotes a binary 1 when a positive frequency deviation occurs from the nominal carrier frequency and conversely, a binary 0, is generated when a negative frequency deviation occurs. Typically, in a Bluetooth radio system, two oscillators will be used to generate this modulation and a two bandpass filter will be used for its demodulation.

Increased data rates of 2Mbps and 3Mbps are now possible using the EDR modulation scheme where the respective rates are achieved through two variants of the PSK. 2Mbps is supported through a π/4 differential quaternary phase-shift keying (or π/4-DQPSK) scheme, which provides us with four phase positions each separated by a 90 degree angle. In comparison the 3Mbps rate is supported with an eight-phase differential quaternary phase-shift keying (8DPSK) scheme. Naturally, this affords us eight phase positions, which are now separated by 45 degrees. Both modulation schemes only affect the carrier and not the frequency, and a PSK receiver device should be capable of distinguishing the type of modulation in order to decode the data. Moreover, each scheme is tolerant to an amount of noise therefore increasing the likelihood of decoding the data more accurately.

Power classes

A Bluetooth-enabled device will support one of the following power classes as defined in Table 11.1. The most common classification is the third, offering an operating distance of up to 1m (~3 feet); typically this is guided by the nominal 0dBm output power requiring a low power consumption of approximately 1mW. In utilizing a frequency hopping scheme (more about this later), Bluetooth is capable of achieving distances of up to 100m (~328 feet) by applying 20dBm to its antenna, although this may require a maximum output power of 100mW, in turn, requiring a larger amount of sourced energy. Power control through these three classes are governed through the *Received Signal Strength Indicator* (RSSI), where the *Link Manager Protocol* (LMP) commands are sent to and from the *Link Manager* (LM) layer to enable regulatory control (increase or decrease) of the transmitter power and, possibly, the level of interference.

If a radio system supports RSSI its accuracy should be ±6dBm. Power control capability is mandatory for a Class 1 device where control can be maintained as low as 4dBm (the maximum output power is 20dBm). The step sequence for regulating power control is maintained in a maximum step of 8dB and a minimum step of 2dB. It is not a mandatory requirement for Class 2 and 3 devices to support power control; nonetheless, it is advisable, as it allows a greater regularity over power consumption and therefore increases battery life.

Bluetooth clock

Each Bluetooth device supports an incremental timing mechanism, which is a free running system. A clock may be implemented as a counter and, as such, a 28-bit variable is required and must wrap around at 2^{28}–1. The *least significant bit* (LSB) increments at 312.5μs per unit which, in turn, provides a clock rate of 3.2kHz. Since the Bluetooth clock is not dependent on the time of day, it can be initialized to

Table 11.1 *The list of power classes and range vs. output power that are available for use within the Bluetooth radio architecture*

Class	Range	Distance	Output Power
1	Long	~ 100m	20dBm
2	Medium	~10m	4dBm
3	Short	~1m	0dBm

Table 11.2 *The Bluetooth clock can appear in several modes and states*

Type	Appearance
CLK	Master Clock
CLK_N	Native Clock
CLK_E	Estimated Clock

any value; typically the clock is initialized to zero. The clock mechanism is used to enable synchronization with other Bluetooth devices, where an offset may be used.

In Table 11.2 we illustrated the various modes and states that the Bluetooth clock can appear. CLK_N is the native clock and is used as the general appearance for all clock references. Typically, the native clock is driven by a *Low Power Oscillator* (LPO) with a tolerance of ±250ppm, but may also be driven by a crystal oscillator with a tolerance of ±20ppm. These modes and states are commonly used for *Standby*, *Park*, *Hold* and *Sniff* modes (more about this later).

Time slots

A Bluetooth clock increments once every 312.5µs, which equates to half a time slot; one time slot therefore equals 625µs. The CLK reference is derived from CLK_N by adding an offset. The CLK_N derivative is used for regulating activities within a piconet, whereas the CLK reference is used for transmission and reception timings. A master of a piconet will have no offset, as the CLK reference is its own native reference. Although, a slave will add an offset to its CLK_N, allowing it to synchronize with the master's native clock; we illustrate this example in Figure 11.2. On a regular basis the slave will need to ensure that the clock is synchronized regularly, as the slave's own clock may drift.

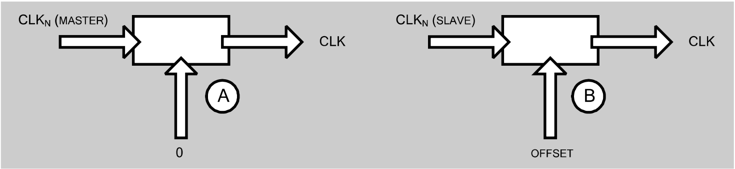


Figure 11.2 *The master maintains its own native clock (CLK) and requires no offset. On the other hand, a slave will synchronize with a master and add an offset to its own CLK_N to enable synchronization.*

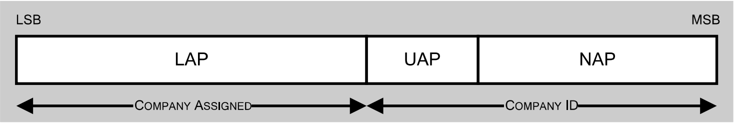


Figure 11.3 *The BD_ADDR is constructed from three fields. The company manufacturing the Bluetooth device assigns the LAP, and the UAP and NAP denotes the company's identification number.*

The mechanisms underlying the synchronization of the clocks ultimately ensures that the master and slave are capable of aligning their transmit and receive slots when exchanging data. It also allows them to determine correct hop sequences, when the frequency channel is pseudo-randomly selected.

Bluetooth device addressing

A unique *Bluetooth Device Address* (BD_ADDR) is assigned to every available Bluetooth-enabled product. The *Institute of Electronic and Electrical Engineers* (IEEE) is responsible for issuing this unique address to manufacturers of Bluetooth-enabled products. It comprises a 48-bit number, which is based on the *Medium Access Control* (MAC) address, notably used for *Network Interface Cards* (NICs). The BD_ADDR comprises three fields: the *Lower Address Part* (LAP) forming 24-bits; the *Upper Address Part* (UAP) forming 8-bits; and the *Non-significant Address Part* (NAP) forming the remaining 16-bits, which we illustrate in Figure 11.3.

The Bluetooth Protocol Stack

The Bluetooth protocol stack is nowadays a tried and tested piece of software and is available from many vendors. The open source solution has also proved to be a popular choice for developers, as it allows a greater diversity in the future development of Bluetooth applications. The stack, like other software stacks presented in the following chapters, is based upon the *Open Systems Interconnect* (OSI) model. You may recall from Chapter 4, *Can we Confidently Rely on Wireless Communications?* we discussed issues surrounding interoperation and highlighted why a stack is architected in this particular manner.

Each layer within the protocol stack has a unique responsibility, which we discuss in more detail in the following sections. In the meantime, Figure 11.4 illustrates the way in which the Bluetooth stack is architected.

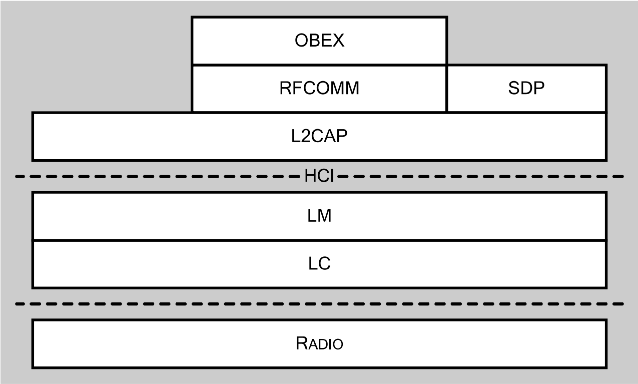


Figure 11.4 *The numerous layers that uniquely form the software building blocks of the Bluetooth protocol stack.*

Link Controller (LC)

Earlier we touched upon the LC layer, which forms the physical layer of our OSI model (Figure 11.1); at this level the layer creates the basic form of physical connection (or channel) between two or more Bluetooth devices. There are various physical channels available and these are illustrated in Table 11.3. A physical channel is characterized by a pseudo-random hopping sequence, which is constructed using the LAP and the UAP of the BD_ADDR. The Bluetooth clock determines the hop sequence for a physical channel, where all channels are subdivided into *time slots*. A time slot governs the organization of packets that are received or transmitted. Depending upon the current state of the Bluetooth device, the maximum number of hop rates per second will vary, that is, 1,600hops/s (*Connection* state) or 3,200hops/s (*Inquiry* or *Page* substates).

A Bluetooth device will support one of two roles when a connection is established with other devices in radio range. A device that initiates a connection is referred

Table 11.3 *The Bluetooth system offers several forms of physical connections between devices in a piconet*

Channel
Basic Piconet Physical Channel
Adapted Piconet Physical Channel
Page Scan Physical Channel
Inquiry Scan Physical Channel

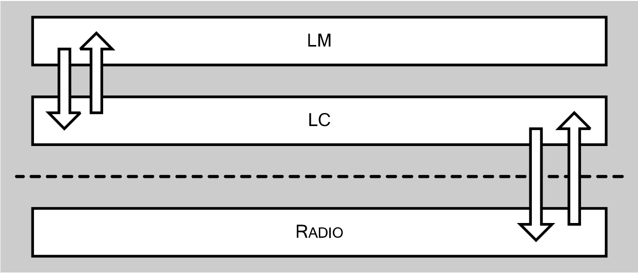


Figure 11.5 *The LC interfaces with the radio's physical architecture and the LM layer, which is denoted by the use of arrows.*

to as a *master* and will be responsible for maintaining a basic piconet physical channel. The end-device will take on the role of *slave*, although once establishment procedures have been made, a role reversal can occur.

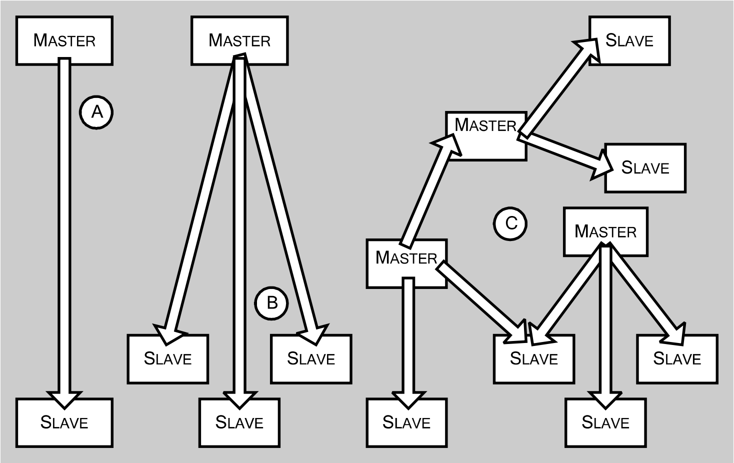
The LC layer (also referred to as the *baseband* layer) is responsible for interfacing with the radio's physical hardware and managing instructions received to and from the LM layer. The LC layer is only concerned with the raw data information received from the LM layer, as it is the responsibility of the upper-layers to interpret and digest the information contained within and to subsequently pass on the data packets to the respective layers. In Figure 11.5 we illustrate a magnified snapshot of the LC layer and its significant interfaces.

The LC layer is also responsible for creating physical connections between point-to-point and point-to-multipoint devices. These configurations are known as master-to-slave and master-to-multi slave configurations and when two or more devices share a physical connection this forms a *piconet*.

In Figure 11.6, the scenarios created by (A) and (B) are piconets, whereas, scenario (C) forms a *scatternet*, this is due to the common devices that are shared by the piconet, although piconets that are not synchronized do not share the same frequency hopping pseudo-random sequence.

At the LC level, data is transmitted to and received from the radio system in a standard packet format; this packet comprises an *access code*, *header* and a *payload*, as illustrated in Figure 11.7. An access code will allow a slave, to determine the source or destination of the originating master device. A slave, for example, will be able to identify the master by its list of addresses stored in its local look-up table, since the access code is generated using the master device's address. The access code field is further broken down into three further fields, comprising a *preamble*, *synchronization*

Figure 11.6 *The various psychical connections available to a Bluetooth device, which is capable of supporting point-to-point and point-to-multipoint configurations.*



word and a *trailer*. The preamble has a fixed 4-bit content dependent upon the start bit of the synchronization word (64-bits). It is primarily used to create a reliable synchronization with the clock of the Bluetooth system in order to collect the rest of the data; the window provided by the system is 5μs. The synchronization word is formed using part of the BD_ADDR. Finally, the trailer follows the synchronization word and comprises 4-bits of fixed information. Again, this is configured depending upon the content of the synchronization word, but will also denote to the rest of the system whether or not a payload will follow.

Before discussing the header field content, we turn our attention to the payload field. This field is optional and, if attached, may contain information pertaining to an instruction, perhaps received from the upper-layers of the protocol stack.

Let us return to our header field; we can see that the header is broken down into six fields, as shown in Figure 11.8. The *Logical Transport Address* (LT_ADDR) comprises a 3-bit field, which denotes an active slave within a piconet (you should note that the master is not assigned a LT_ADDR).

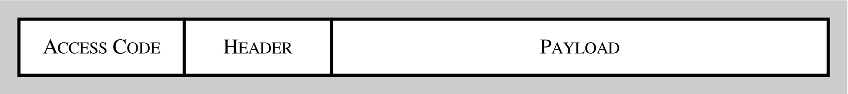


Figure 11.7 *The standard data packet used at the LC level comprises an access code, header and a payload. This standard packet will be used to encompass data to and from the upper-layers of the protocol stack.*

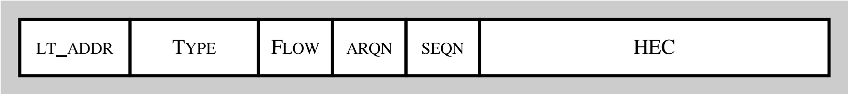


Figure 11.8 *The header of the standard packet is constructed with six fields.*

Several types of transport designations may be created between a master and slave; each type of available transport has been identified in Table 11.4. The SCO, eSCO and ACL are logic point-to-point transports between a master and slave device whereas the ASB is used when a master wishes to communicate with many active slaves whilst the PSB allows the master to communicate with many parked slaves.

Link Manager (LM)

The LM layer is concerned with establishing connection set-up and to ensure that both or more parties are authenticated (if required). Additionally, it is also responsible for establishing encryption on the communications link. The LM layer uses a well-defined protocol, which is referred to as the *Link Manager Protocol* (LMP), to achieve connection set-up, authentication and encryption; the protocol is a defined set of instructions or messages known as *Protocol Data Units* (PDUs) that successfully enable the peer-to-peer connection set-up between two or more Bluetooth-enabled devices. In Figure 11.9 we illustrate the interfacing layers to which LM communicates to and from. When exchanging messages to its peer, the default ACL logical transport (see Table 11.4) is used. More specifically, the ACL-*Control* (ACL-C)

Table 11.4 *There are five types of logical transport addressing what can be created between a master and slave device*

Logical Transport	Acronym
Synchronous Connection-Orientated	SCO
Extended Synchronous Connection-Orientated	eSCO
Asynchronous Connection-Orientated	ACL
Active Slave Broadcast	ASB
Parked Slave Broadcast	PSB

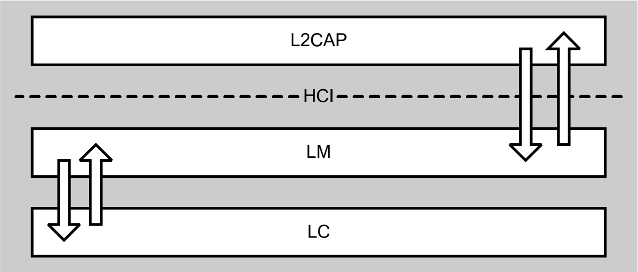


Figure 11.9 *The LM interfaces with the LC layer and may interface with a Host Controller Interface.*

logical transport is used and has the highest priority than any other traffic; similarly, *Logical Link Control and Adaptation Protocol* based (L2CAP-based) messages are denoted as ACL-*User* (ACL-U) to prescribe the specific user or L2CAP-specifc data being sent by the L2CAP layer (more about this later). In short, ACL-C data is sent to and received from the LC layer whereas ACL-U data is sent to and received from the L2CAP layer.

The LM layer uses a wealth of PDUs, which enables certain behavioral characteristics within the Bluetooth device. Typically, a PDU will contain a 7- or 15-bit *Operations Code* (OpCode), which is used to distinguish the type of PDU being transmitted. In Table 11.5 we identify three of the seventy or so operational codes that may be used when establishing characteristics and features within a Bluetooth-enabled device.

The LM layer operates its protocol as a transactional topology, that is, a request/response paradigm, in that when a request is made it expects a response, allowing the LM layer to determine the success or failure of a request and if it needs to undertake further action. For example, the `LMP_host_connection_req` in Table 11.5 may receive an `LMP_accepted` or `LMP_not_accepted` PDU where the LM layer can then take appropriate action. In Figure 11.10 we illustrate the payload of a 7-bit OpCode PDU. The *Transaction ID* (TID) occupies the first bit in the OpCode and if set to 1 (one), denotes that the transaction was initiated by slave where 0 (zero), denotes that it was initiated by the master.

Host Controller Interface (HCI)

The HCI is not a layer as such within the Bluetooth protocol stack. It is an interface that permits the host and host controller to communicate with each other. In some

Table 11.5 *A small set of PDUs that help facilitate the connection characteristics and features of a Bluetooth-enabled device*

PDU	OpCode	Description
LMP_host_connection_req	51	The PDU that is used to request a connection with a peer device.
LMP_accepted	3	This PDU denotes that the LMP_host_connection_req was successful and the connection can be established.
LMP_not_accepted	4	This PDU denotes that the LMP_host_connection_req was unsuccessful and the connection cannot be established.

Bluetooth implementations some manufacturers may wish to separate the host and host controller functionality and, as such, there has to be a means by which these two very separate components of the Bluetooth system communicate. In demonstrating the difference between the host and host controller, we can attribute the host controller comprising the radio, LC and LM software, as shown in Figure 11.11. If we imagine that this forms our USB or PCMCIA Bluetooth device, which we have to insert into our notebook to enable Bluetooth functionality. The operating system, running on our host, for example, Microsoft Windows or Linux, will contain the rest of the Bluetooth protocol stack above the HCI; in particular, L2CAP, RFCOMM, SDP and so on. The connection made by the USB or PCMCIA device to the host forms the interface between our host and host controller. As such, the Bluetooth specification defines four such possible interfaces, as shown in Table 11.6.

The UART transport layer supports a serial interface between two UART devices and support four different types of HCI packets, namely *Command*, *Event*, *ACL* and *SCO* data packets. A command/event paradigm is supported in that when a command is issued an event is expected as its outcome. In comparison the ACL and SCO data packets can be sent freely to and from the host controller. The 3Wire UART transport

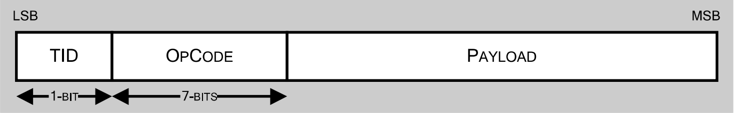


Figure 11.10 *The depiction of a payload when a 7-bit PDU transaction is being exchanged.*

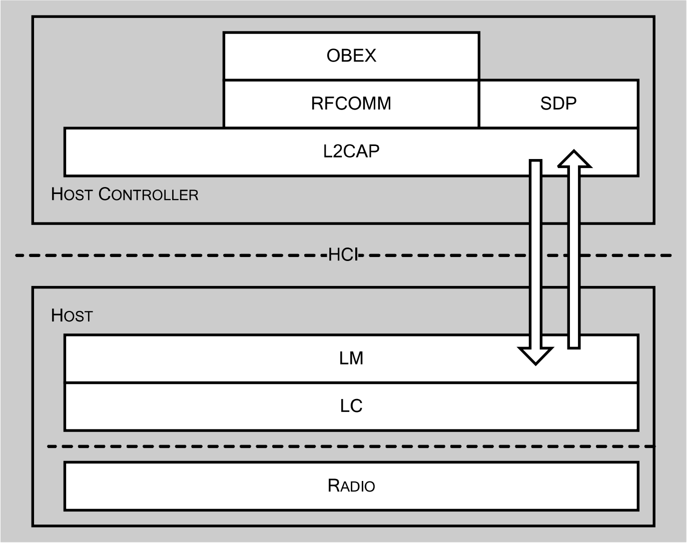


Figure 11.11 *The separation that occurs when manufacturers separate the host and host controller. The HCI is used to enable these two components to communicate with each other.*

layer differs to the UART layer in that it is capable of communicating between two UART devices. In this particular instance a connection-based communication link is established to deliver the same HCI packets. It differs in that a packet header is appended to the payload and the data is formatted with a *Serial Line Internet Protocol* (SLIP). The purpose of this particular method of communication is to provide some assurance with data transmission over the UART interface, as the original UART did not detect errors or erroneous data packets.

The SD transport layer is primarily used for interfacing memory card type applications and is well specified in the *Secure Digital IO* (SDIO) specification, which is

Table 11.6 *The four HCI transport mechanisms that enable the host and host controller components of a Bluetooth system to communicate with each other*

Interface	Description
UART	Universal Asynchronous Receiver Transmitter
3Wire UART	3Wire Universal Asynchronous Receiver Transmitter
SD	Secure Digital
USB	Universal Serial Bus

available via the *Secure Digital Association* (SDA) website (www.sdcard.org). And finally, the *Universal Serial Bus* (USB) transport layer prescribes the functionality and behavior that is expected by the layer to enable a host and host controller to communicate via a USB interface. Now that we have established how communication is achieved between a host and a host controller we can begin to explore the higher-level Bluetooth protocol layers.

Logical Link Control and Adaptation Protocol (L2CAP)

The L2CAP layer forms the data link layer of our OSI model (back in Figure 11.1). Its purpose is to provide a connection-orientated and connectionless service to the higher-layers within the Bluetooth protocol stack. More specifically, it provides protocol/channel multiplexing, *segmentation and reassembly* (SAR) and group abstractions. In a similar fashion to LMP, L2CAP distinguishes between data flow within its layer and, as such, a *Service Data Unit* (SDU) is used to transport data to and from the upper-layers of the Bluetooth protocol stack; and L2CAP PDUs carry data relating to the upper-layers or may contain L2CAP-specific protocol information. In establishing communication with the upper layers, as shown in Figure 11.12, the L2CAP layer uses the notion of *channels* and for each logical channel endpoint of a channel, a unique *Channel Identifier* (CID) is used. What it enables the L2CAP layer to do, is to associate itself with the peer entity of the logical channel that is associated with a particular device. It primarily serves the interface of the host controller to the application residing on the host.

Service Discovery Protocol (SDP)

The SDP is provided to enable other devices that may be interested in learning of other devices in proximity. In Figure 11.13 we illustrate that the SDP interfaces with

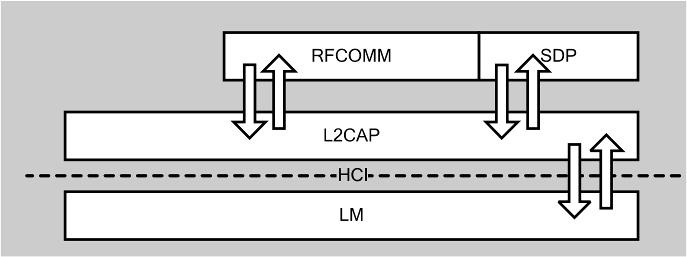


Figure 11.12 *The L2CAP layer interfaces with the RFCOMM and SDP layers (additionally, the L2CAP layer interfaces with the TCS layer, which is not shown here).*

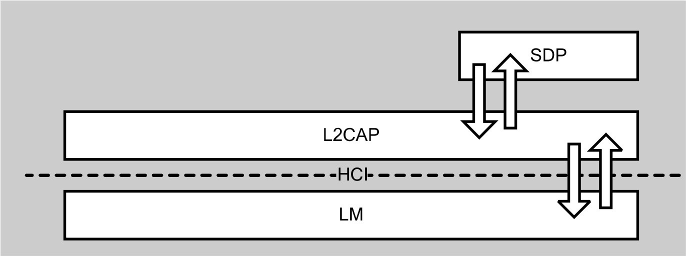


Figure 11.13 *The SDP layer relies on the interface provided by the L2CAP layer to achieve peer-to-peer connectivity.*

the higher layers and extends an interface to the L2CAP layer allowing it to communicate with its peer. It allows the inquiring device to discover specific features and capabilities of the device in proximity, such as, specifics profile it may support. In essence it supports an holistic and impartial insight into the available services of other Bluetooth-enabled devices. Consumers then may choose to interoperate with that device if it actually offers a service that it wants. SDP uses a series of PDUs in a command/response paradigm to facilitate in establishing and discovering available Bluetooth services.

RFCOMM

The RFCOMM layer is responsible for providing serial port emulation and is illustrated in Figure 11.14. Its purpose is primarily to support a host of Infrared legacy applications and can support up to sixty simultaneous connections, although this remains implementation dependent. In a peer-to-peer topology it's as if the two entities are mimicking (emulating) a physical serial connection, which includes the various RS232 Control Signals, as well as providing null modem support.

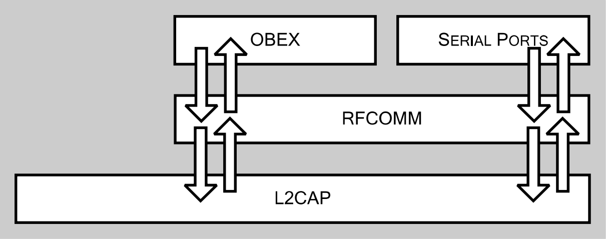


Figure 11.14 *The RFCOMM layer exposes a serial connection to the OBEX layer and provides support to a host of Infrared legacy applications.*

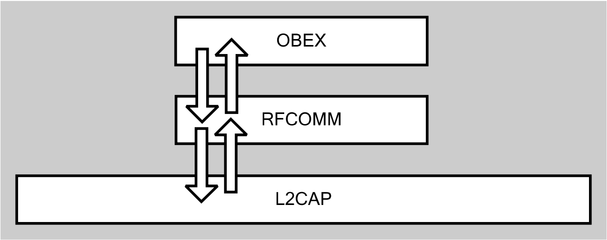


Figure 11.15 *The RFCOMM layer supports emulated serial port capability, in turn, allowing OBEX to support a host of Infrared legacy applications.*

Object Exchange (OBEX)

The RFCOMM layer emulates serial port capability and, as we highlighted, it supports a host of Infrared applications. The OBEX layer is specifically concerned in realizing these applications which, in turn, enables the IrDA protocol to run over the Bluetooth protocol stack, as shown in Figure 11.15.

The OBEX layer is not limited to support serial-based communications either, the Bluetooth specification also discusses the possibility of supporting OBEX over TCP/IP, but does not explicitly define how you should implement TCP/IP over Bluetooth. The OBEX layer prescribes in particular, three use cases, namely *Synchronization*, *File Transfer* and *Object Push*. These applications are historically based within the Infrared protocol and it is surprising, even today, how many Bluetooth-enabled devises do not support this basic functionality.

What are Bluetooth Profiles?

Many people can describe a Bluetooth Profile as the *Generic Access Profile* (GAP) or the *Headset Profile* (HP), but fail to understand its purpose. A Bluetooth Profile is a specification that specifies how a particular application should behave; what characteristics in terms of functionality should an application exhibit, that is, explicit function expectations from the lower-layers of the Bluetooth protocol stack; and how should this functionality manifest itself to the user interface, in turn, the user. It establishes commonality in terminology that is used across all applications, such as Bluetooth Passkey, Pairing and so on. And, it remains pivotal in establishing a single representation of the functionality that may be exhibited by a Bluetooth-enabled product or application.

Extending the application-base

With an already established range of applications (Bluetooth Profiles) and the potential forthcoming application base when the marriage of Bluetooth and UWB has been consummated, then there is clearly an opportunity for many individuals and manufacturers to develop new applications. Furthermore, the current specification is being upgraded to reflect new changes to the core specification and new profiles. A change is inevitable as we see the marriage of Bluetooth and UWB evolve from its flimsy paper anniversary to a more solid foundation that may become wood denoting five years of a successful relationship. Naturally, with an established relationship there's always the possibility of complacency and the allure of a seven year itch. Fortunately the Bluetooth SIG, an incorporated organization responsible for architecting and shaping Bluetooth's future, creates a series of *Marketing Requirement Documents* (MRDs) that disclose future usage scenarios. These MRDs are the foundation from which the specification has evolved and further MRDs are created to provide new usage scenarios, that is, new ideas that may result in new applications (or profiles). You may consider the MRD, as an internal business justification process within the SIG; these usage scenarios are submitted to external reviewers for their comments.

Foundation Profiles

The following table (Table 11.7) lists the original set of Bluetooth profiles proposed in the Specification of the Bluetooth System: Profiles, v1.1. Incidentally, the *LAN Access Profile* (LAP) has been disbanded and is now replaced with the *Personal Area Networking* (PAN) Profile. The number of profiles outlined in this table are prevalent in most Bluetooth wireless products and have enjoyed a moderate success within the Bluetooth community.

The Adopted Profiles

The adopted profiles (as shown in Table 11.8) are a clear diversification from the founding profiles, perhaps an acknowledgement to the SIG that it needs to adapt its current application portfolio to a more multimedia-centric application base, which (we are told) the consumer desperately needs to fulfill.

Table 11.7
A full list of the available foundation profiles that forms the initial presentation of the draft and subsequent public release of the Specification of the Bluetooth System: Profiles v1.1

Profile	Acronym
Generic Access Profile	GAP
Service Discovery Application Profile	SDAP
Cordless Telephone Profile	CTP
Intercom Profile	ICP
Serial Port Profile	SPP
Headset Profile	HSP
Dial-up Networking Profile	DUN
Fax Profile	FAX
LAN Access Profile	LAP
Generic Object Exchange Profile	GOEP
Object Push Profile	OPP
File Transfer Profile	FTP
Synchronization Profile	Synch

Table 11.8
A summary of the adopted profiles. Many new profiles are on their way.

Profile	Acronym
Advanced Audio Distribution Profile	A2DP
Audio/Video Remote Control Profile	AVRCP
Generic Audio/Video Distribution Profile	GAVDP
Video Conference Profile	VCP
Video Distribution Profile	VDP
Press-to-talk in the Hands-free Profile	PTTinHFP
Message Access Profile	MAP
Phone Book Access Profile	PBAP
SIM Access Profile	SAP
Human Interface Device Profile	HID
Common ISDN Access Profile	CIP
Extended Services Discovery Profile	ESDP
Basic Printing Profile	BIP
Hardcopy Replacement Profile	HCRP
Basic Printing Profile	BPP
Personal Area Networking Profile	PAN

Table 11.9 *A summary of the new protocols which provide the foundation to a number of adopted Bluetooth Profiles*

Protocol	Acronym	Version
Audio/Video Control Transport Protocol	AVCTP	v1.2
Audio/Video Distribution Transport Protocol	AVDTP	v1.2
Bluetooth Network Encapsulation Protocol	BNEP	v1.0

New Protocols

In a need to evolve and provide better use cases, the Bluetooth SIG have architected additional protocols that underlie a new range of profiles, as illustrated in our previous section. You will notice that a significant number of protocols now surround the audio/video-base of applications, as shown in Table 11.9.

Conclusion

The furor and the push into a wireless existence for the consumer perhaps stems from the plethora of Bluetooth applications and a vision of Bluetooth wireless technology that seems to have been muted. But, what happened? Who tripped along the way and shattered a vision that was perceived to be all clear and all knowing? At one point in time, Bluetooth was accused of being the “jack of all trades” and “master of none.” And, perhaps it was also guilty of losing its path, its direction of the basic premise, in that it was merely a cable replacement technology. Today, it seems to have been demoted to a technology that merely serves a cable replacement for a cellular phone and its headset and perhaps the automobile. Its destination and future is still unclear, at the time of writing, even with its recent alliance with UWB, which to be honest seems a desperate endeavor to hold on to a dream of sustaining dominance.

Bluetooth wireless technology needs a type of genius that allows it to sustain a perception of need and this may have been successfully portrayed in a US advertisement of a very well-known brand of consumer electronics. In the advert we see a small girl preparing herself for her first stage performance. In her excitement she continually seeks the approval of her parents who are filming the event. It appears that the girl seems to be upset as she assumes her parents who are set away back from the stage will not be able to effectively capture her performance. But, upon arriving home, the family view the film together and the little girl is astonished and excited when she perceives the film to be singularly about her, as all you can hear is the little girl’s dialogue.

With the simplicity afforded by a Bluetooth microphone wirelessly connected to the handheld video camera we can capture the imagination, and the wallets, of those parents who have found themselves in a similar situation and, in turn, attempt to increase our consumer-base of Bluetooth-enabled technology.

You may have witnessed the shift in many founding pioneers of the Bluetooth era to establish a more open and diversified wireless portfolio where they may now provide silicon for multiple wireless technologies, as they daren't put their clichéd "eggs into one basket." UWB as a technology in its own right would have succeeded and, as Andrew Carnegie said, "and while the law (of competition) may be sometimes hard for the individual, it is best for the race, because it ensures the survival of the fittest in every department" and, it is with no doubt, that we would have seen the demise of Bluetooth.

Summary

- With the new release of the Specification of the Bluetooth System and the many adopted profiles, we will surely see an emerging wealth of detailed information.
- The release of the Specification of the Bluetooth System: Core v2.0, plus EDR offers backward compatibility with v1.2.
- We already have a series of adopted profiles that have been prepared and incorporated into a formal release.
- With the recent marriage of Bluetooth and *Ultra-wideband* (UWB) we may even witness a new evolution to the specification suite; perhaps we will see *Specification of the Bluetooth System: Core v3.0* with an accompanied wealth of new profiles.
- This continued growth is evidence of a technology that has taken up permanent residence in communication-enabled products, albeit predominantly targeted towards the cellular market.
- Bluetooth wireless technology's success is evident in the cellular market.
- Indeed, this is further heightened in the UK, the US and, similarly, other European countries where local and/or national Governments have made it an illegal offence to operate a cellular phone within a vehicle.
- Drivers are only allowed to operate hands-free devices.
- Those caught holding a cellular phone within their vehicle will receive an on-the-spot fine and will automatically accrue numerous penalties.
- The momentum of Bluetooth wireless technology is accelerating at a phenomenal rate within applications surrounding the cellular and audio market.

- In the UK, Europe and increasingly the US, many consumers have chosen to interoperate their cellular phone with a Bluetooth-enabled headset.
- With an increase in popularity of Apple's iPod generation of products, a somewhat natural evolution to the headset is to support wireless stereo functionality.
- Bluetooth technology has its application-base firmly founded in Infrared.
- Even today, manufacturers have not abandoned this tried and trusted technology.
- The sheer simplicity of Infrared conveys a degree of confidence that has been unmatched by any other wireless technology to date.
- The founding premise of Bluetooth is that you no longer need to point at a device to make it do something.
- Bluetooth now needs to encompass a wider market and maintain the offer of simplicity for it to succeed.
- What is to be made of the newly formed alliance between Bluetooth wireless technology and UWB?
- It is clearly evident that UWB offers higher data rates and establishes a more reliable data connection.
- Many have argued that Bluetooth and UWB are competitors.
- On numerous occasions we may have become privy to use cases illustrating how it would be possible for UWB to succeed where Bluetooth fails.
- Some reports even dare to suggest that Bluetooth is dead.
- It seems that, with a degree of predictability, following various announcements made by the Bluetooth SIG and press agencies, industry commentators have unconditionally welcomed the extensible possibilities that UWB offers Bluetooth.
- It is painfully clear that without such support from the wider industry Bluetooth would have surely suffered disbandment along with HomeRF.
- It is envisaged that UWB will be architected within the Bluetooth specification, in turn, enabling the much sought after higher data rates and the ability to penetrate popular audio/video types of applications.
- It has to be said that secretly Bluetooth has also been viewed by many in the industry as a technology struggling to penetrate key products within the consumer electronics market.
- What is more evident is the poor uptake of Bluetooth in mainstream consumer electronics within the US and to a greater extent in the UK and Europe.
- This is rumored to be poor interoperation and coexistence related issues.
- With an incredible foresight, the Bluetooth SIG have refused to become stagnant in a market that demands change and expects improved functionality.

- The SIG have been pushed into introducing modifications that have afforded it efficient discovery and pairing procedures, as well as modifying the most critical aspect: coexistence.
- In introducing the AFH scheme Bluetooth provides a more harmonious coexistence with the large consumer base of proprietary and standardized wireless technologies.
- The marriage of Bluetooth and UWB can now realistically push a new generation of technology that will serve the WUSB dream much more satisfactorily.
- When you compare Bluetooth's EDR offering data rates of up to 3Mbps and compare that with UWB's offering of up to a theoretical 1Gbps you may begin to understand the range of possibilities.
- It seems that UWB is riding Bluetooth's already established market acceptance and through a back door we will undoubtedly witness UWB become the basis of most Bluetooth audio/video solutions.
- The combination of UWB and Bluetooth technologies has manifested itself into a categorization known as WiMedia.
- It seems that a full and final definition of what WiMedia is remains somewhat elusive.
- Many articles refer to several personal-area wireless technologies arguing that each uniquely affords its own make-up of what WiMedia can do.
- If you refer to the WiMedia Alliance's website they seem to portray an image of unison between UWB and Bluetooth, supporting a genre of multimedia-centric applications for the consumer electronics industry.
- Ironically, it has taken the consumer a good number of years to understand what Bluetooth supports and now they have to ingest yet another wireless technology.
- It is clear that the collective spectrum offered by UWB and Bluetooth will be seen as WUSB and should afford a more harmonious introduction to the consumer.
- At one point in time, Bluetooth was accused of being the "jack of all trades" and "master of none."
- Today, it seems to have been demoted to a technology that merely serves a cable replacement for a cellular phone and its headset.
- Its destination and future is still unclear, even with its recent alliance with UWB, which to be honest seems a desperate endeavor to hold on to a dream of sustaining dominance.
- Bluetooth wireless technology needs a type of genius that allows it to sustain a perception of need.
- With the simplicity afforded by some Bluetooth applications we may capture the imagination, and the wallets, of a new consumer-base.

- You may have witnessed the shift in many founding pioneers of the Bluetooth era to establish a more open and diversified wireless portfolio.
- They may now provide silicon for multiple wireless technologies, as they daren't put their clichéd "eggs into one basket."
- UWB as a technology in its own right would have succeeded and, in a battle of survival of the fittest, it is with no doubt that we would have seen the demise of Bluetooth.

12

ZigBee: Untethered and Unlicensed

The ZigBee Alliance (www.zigbee.org) ratified its standard wireless technology (v1.0) in December 2004 (made it public in June 2005) and is now finalizing v1.1, which takes advantage of the enhancements that were made to the 802.15.4 specification, namely some improved authentication and encryption features; there are some other additional improvements which we'll touch upon in a moment. The new revision of the specification will be available at the end of 2006, start of 2007, but it is unclear as to who will be watching this damp squib. Naturally, v1.1 will address the plethora of errata that has already been generated, but it's also uncertain as to whether or not backward compatibility can be achieved and we will no doubt hear uniformed tutting amongst the initial pioneers who dared to venture into an unknown wireless domain. In fact, ZigBee seems to lack a basic feature set that so many other wireless technologies offer as a founding step forward – you only have to compare it to Z-Wave (from Chapter 7, *ZenSys: An Open Standard for Wireless Home Control*), to appreciate the chasm between them. And, it seems that a significant number of the initial promoter companies are already abandoning ship; it really doesn't bode well for the future of ZigBee. You are undoubtedly already aware that ZigBee is targeted to populate the home and office environment, offering low power solutions for toys, peripherals, control, security and monitoring type applications. The technology itself received an ambivalent response from manufacturers and the press alike, and its acceptance still remains somewhat muted. Many have argued that the need for the technology is futile, in the wake of other well-established technologies such as Bluetooth (Chapter 11, *Bluetooth: A Cable Replacement Technology*), Z-Wave (Chapter: 7, *ZenSys*: *An Open Standard for Wireless Home Control*) and WiFi (Chapter 13, *WiFi: Enabling True Ubiquitous Connectivity*); more specifically, the apathy centered on a number of proposed alternatives. During the time ZigBee was being conceived, Bluetooth had already enjoyed some moderate success. The relationship between them might be likened to that of your younger sister receiving wrenching parental-overtones informing her that she was an accident, "We only wanted the one!" *Bluetooth Lite* was put forward as an alternative to ZigBee and, as such, ZigBee in its fetus-like state should perhaps have been aborted. Bluetooth and its pomposity failed to clone a sibling comparable to ZigBee's genetic base and today still remains a classic fable. Bluetooth Lite, the would-be derivative of the original specification, with its promised optimized *Media Access Controller* (MAC) should have naturally made ZigBee a regrettable mistake, but things do work out for the best and curiously, what did become of ZigBee's big brother? It was some time ago when Ericsson Technology Licensing withdrew its interest from core Bluetooth development, causing tremors within the Bluetooth community that exceeded any known Richter scale. We are all aware that Ericsson founded and directed the Bluetooth technology and remains a proponent company in Bluetooth's future. However, the momentum behind Bluetooth Lite wavered and disinterest dominated the rigmarole of enduring yet another spat at defining a cholesterol-free technology. It is evident that Bluetooth Lite suffered a well-known syndrome called hyperbole – a symptom that can only be attributed to the fervor surrounding Bluetooth wireless technology at that time. After all, we did concede in our earlier chapter (Chapter 11) that Bluetooth was "jack of all trades" and "master of none."

With the continuing changes being made to the 802.11 specification and the increased deployment and success of WiFi technology, we have witnessed an unfathomable adoption of a wireless technology populating the home and office environment; hence making the choice for ZigBee somewhat redundant, as with more cost effective solutions for WiFi and a decrease in power consumption, WiFi at first glance appears to be a more obvious choice, even for the most basic of wireless applications. But alas, WiFi is quite simply overkill for applications such as toys, monitoring, control and so on; not just in terms of its data throughput, but moreover its application (software) base. Unlike Bluetooth Lite, low power WiFi is not a fable, it is a definite reality. In establishing a successful technology like WiFi, silicon vendors and the WiFi Alliance (www.wi-fi.org) have consorted to overcome issues surrounding power consumption in smaller devices, such as cellular phones, *Personal Digital Assistants* (PDAs) and MP3 players. Their resulting effort is *WiFi Multimedia* (WMM) Power Save, which we discuss in more detail in Chapter 13, *WiFi: Enabling True Ubiquitous Connectivity*. The WMM Power Save is a set of features that have evolved from legacy power save technology (already within numerous 802.11b-enabled products) in combination with a number of attributes within the 802.11e standard. The basic premise of the power save mechanism is its optimized data transmission technique, in that a data stream is transmitted in the shortest period of time, in turn, encouraging the device to remain asleep for as long as possible.

Comparing ZigBee and Z-Wave

If you have read Chapter 7, *ZenSys: An Open Standard for Wireless Home Control*, and you are now embarking up on this chapter, you may be conscious of the considerable overlap between the technologies (ZigBee and Z-Wave). In fact, Zensys (www.zen-sys.com), the Danish company that develops the Z-Wave technology, was formally part of the ZigBee Alliance, but differences between their business models and technology approach created a rift between the Alliance and Zensys. As such, Zensys withdrew its support from the Alliance and essentially formed their own Z-Wave Alliance (www.z-wavealliance.org) group that today has over one hundred members, which is comparable to that of the ZigBee. Furthermore, there isn't a great difference between the two technology solutions. Both technologies support the notion of nodes and indeed support the same networking topologies (more about this in a moment) and essentially the same application portfolio is again supported by both Z-Wave and ZigBee. But Zensys has a clear advantage, as it has already established within the market a large consumer base of home control and automation products which, to be honest, ZigBee has yet to do. Additionally, Z-Wave is increasingly being seen as the de facto standard for wireless home control and automation solutions, which surely must have ZigBee feeling somewhat insecure. It is primarily due to companies and technologies like Zensys which are analogous to ZigBee that so many argued that the emergence of yet another home control-like technology was pointless.

Our Reasons to Believe

Despite a stay-of-execution, the ZigBee Alliance has persevered and released their initial specification for the technology world to see and it continues to evolve the technology. Can a passion that is untethered and unlicensed summon the vision required to realize a new way of interoperation and wireless capability, or will it be relegated to classic wireless history? In allowing the technology a measured opportunity to thrive, we may have to concede to the possibility that the second edition of this book shall retain the chapter title "ZigBee: Untethered and Unlicensed," but underneath it will merely read "this page has been intentionally left blank." Only time will afford us hindsight.

ZigBee's inception is derived from a notion of *simplicity*. When we compare other standards-based wireless technologies, they tend to be larger, in software and hardware implementation terms, and consume more (battery) power. Although, it is unclear at this time if ZigBee will actually achieve its marketed consumption statistics in addition to truly realizing a small software implementation. The aforementioned technologies, Bluetooth and WiFi, are indeed excellent examples, which continue to promise better, more cost effective, power efficient models and fruitful application use cases. Similarly, their networking topologies can at times become cumbersome to implement and understand. WiFi is building upon the success of its 802.11b userbase where we see new emerging standards that provide scenarios offering backward capability (with 802.11g), ad-hoc and *mesh* networking (more about this in a moment). Likewise, Bluetooth technology with its existing topology of a piconet is further being enhanced to ensure better reliability and usage scenarios when creating scatternets (multiple interconnecting piconets).

The foundation on which ZigBee is derived is a cost effective wireless model that the ZigBee Alliance hopes will become a de facto standard for low-cost wireless technology solutions. With its low data rate and simple to implement protocol realizing a multitude of applications (or profiles) we ultimately witness a technology that has been developed and targeted to do a job.

ZigBee's Networking Topology

ZigBee's topology is essentially a simple one to understand; we illustrate three topologies in Figure 12.1 and Figure 12.2. Numerous *nodes* are strategically deployed in an area, typically a home or office, where the radio coverage of one node overlaps an adjacent node. This enables the possibility of one reaching another even if they are thirty meters (100 feet or so) apart. In a relay style race the baton (data) is passed from one node to another until the destination node is reached. ZigBee's *networking* (NWK) philosophy offers three topologies, namely the *star*, *mesh* and *tree*, as we already indicated and are application dependent. The star implementation offers an application a

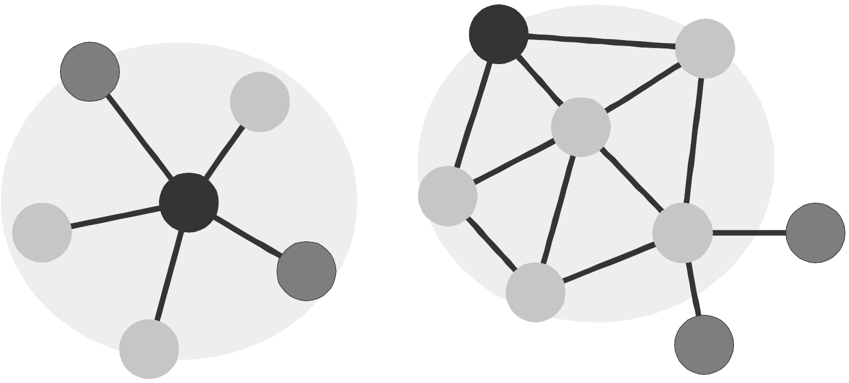


Figure 12.1 *Two of the three networking topologies offered by ZigBee; (a) the Star topology and (b) the Mesh topology.*

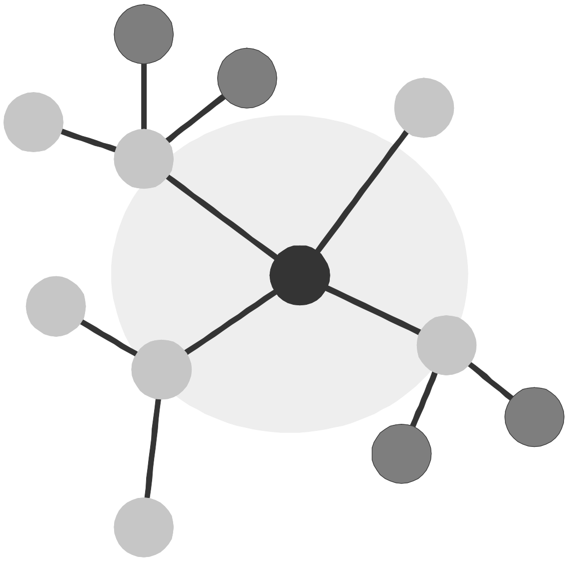


Figure 12.2 *The third networking topology offered by ZigBee: the Tree topology.*

Personal Area Networking (PAN) context, in that only one *coordinator* node is responsible for all communications. In comparison, a mesh implementation affords the application an *end device*, which may take the form of a *full function device* (FFD) or *reduced function device* (RFD). Finally, the tree topology is capable of extending the star topology. In particular, what we create here is multiple star topologies where an RFD is replaced with an FFD, in turn, enabling another star network to be attached. The resulting ZigBee network can be extended over an unlimited geographical location (okay, let's keep that in perspective; we are not talking continents, but office or living room space). Incidentally, we have innocuously depicted three major device types within the ZigBee network; more specifically, we have a *coordinator*, an *end device* and a *router*. Curious, when did the router device emerge? You may recall, in our relay style race, that data is moved from node to node and, as such, it is the responsibility of the router to ensure that an end device (FFD or RFD) receives the initiating data from the controller. The controller has the responsibility for creating and maintaining connections throughout the ZigBee network. There are specific application-dependent limitations, but in essence we are not a million miles away from where we need to be.

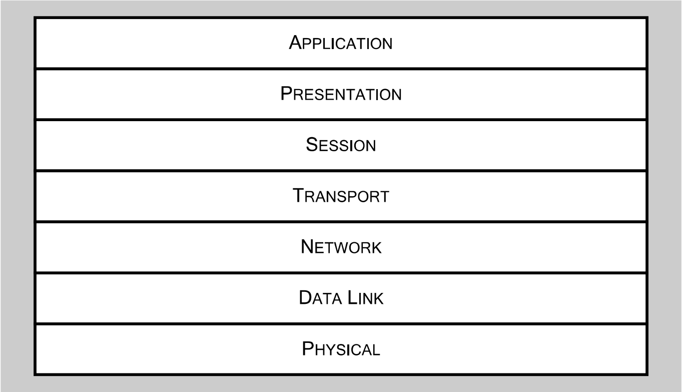
Additionally, you should also be aware of *beacons* (also *non-beacons*). ZigBee affords two network configuration-specific channel access schemes. In the non-beacon channel access mode the ZigBee network uses an unslotted *Carrier Sense Multiple Access with Collision Avoidance* (CSMA-CA) technique. You may recall we touched upon this technique in Chapter 4, *Can we Confidently Rely on Wireless Communication?*

where we discussed issues of multiple ZigBee-enabled devices in proximity communicating at the same time. Essentially, a ZigBee node will wait a random period before transmitting on a particular channel; if the channel is idle, the node can transmit its data, otherwise it has to wait again (the same random period) before it makes another attempt. In a beacon channel access mode, typically ZigBee routers that are not part of a mesh network environment are only required to receive data when data is being transmitted. The period in which these beacons become active is reduced and, as such, decreases their duty cycle or in other words, the longer they remain inactive ultimately extends their battery life.

The Radio Architecture

With a good foundation of the networking infrastructure and established way-of-working, we can embark upon understanding ZigBee's radio architecture. In Figure 12.3 we illustrate the *Open Systems Interconnect* (OSI) model, which forms the basis of the many wireless protocol stacks and, indeed, ZigBee is no exception. In particular, the data link or *medium access control* (MAC) and physical (PHY) layers are defined by the *Institute of Electrical and Electronic Engineers* (IEEE) 802.15.4 specification; whereas, the layers above it are within the domain of the ZigBee Alliance. Again in Chapter 4, *Can we Confidently Rely on Wireless Communication?* you may recall that we discussed issues surrounding coexistence and touched upon the various spectrums that ZigBee used. In fact, ZigBee provides three *Industrial Scientific and Medical* (ISM) bands, namely 868MHz for Europe; 915MHz for the United States, and 2.4GHz for world-wide usage. ZigBee radios use *Direct Sequence Spread Spectrum* (DSSS). This, in turn, affects how channels are allocated in the respective frequencies: 868MHz (one channel);

Figure 12.3
The OSI model which, to a large extent, remains common to all wireless protocol stacks.



915MHz (ten channels) and 2.4GHz (sixteen channels). The spread-spectrum nature of the modulation technique offers a transmission that covers the full spectrum which, in turn, prescribes the number of available channels within the radio band. The IEEE 802.15.4 specification offers two modulation schemes which depend upon the actual radio band being used. In the instance where 868MHz and 915MHz bands are used then the IEEE 802.15.4 specification utilizes the *Binary Phase Shift Keying* (BPSK) digital modulation scheme. In this context the data rate achieved for 868MHz usage is a theoretical 20kbp/s and 915MHz usage is approximately 40kbits/s. The 2.4GHz scheme utilizes an orthogonal *Quadrature Phase Shift Keying* (QPSK) modulation scheme, which helps ZigBee to achieve a theoretical data throughput of 250kbits/s.

Security and authentication

The ZigBee network is very secure; it uses an access control list only allowing known-nodes to enter the network. And, authentication is assured by preventing devices from impersonating other devices by using a common network key and establishing unique keys between device nodes. Additionally, the 802.15.4 specification offers additional security features assuring users that their network is safe from intruders. Furthermore, ZigBee uses the 128-bit *Advanced Encryption Standard* (AES) algorithm, which discourages would-be eavesdroppers and a refresh message timer. The refresh timer overcome replay attacks as a message has a certain window of time to reach a node and, as such, if the message reaches the node after this window, it is rejected.

Coexistence and interoperability

In an open standard such as ZigBee, interoperation is encouraged through the use of adopting a common platform upon which to develop wireless applications. You may recall from Chapter 4, *Can we Confidently Rely on Wireless Communication?* we discussed in some detail how a protocol stack is used to ensure functionality at the right layer in a peer-to-peer fashion. And, as we have already discussed, CSMA-CA is used to ensure successful coexistence with ZigBee devices and other similarly-enabled devices in the same environment.

802.15.4: Low data rate, low power Wireless Personal Area Network (WPAN)

The IEEE 802.15 working group comprises five subsets of task groups, which specializes in a given *Wireless Personal Area Network* (WPAN) domain, as we illustrate in

Table 12.1 *The five task groups within the 802.15 working group that specializes in a particular wireless personal-area network domain*

Group	WPAN Domain
1	Bluetooth
2	Coexistence
3	High data rate
4	Low data rate
5	Mesh networking

Table 12-1. Incidentally, task group 1 has undertaken effort to produce a WPAN standard based upon Bluetooth (v1.1) and in a similar manner to ZigBee the specification merely covers the PHY and MAC layers.

In our earlier introduction we mentioned that the new revision of the ZigBee specification (v1.1) will take advantage of the modifications that were made to the original 802.15.4 specification. You may often see this specification being referred to as 802.15.4-2003, which represents the year in which the specification was released. It may be evident that task group 4 is involved in defining the future of this standard. Within this task group there are further modifications that have been made to the original 802.15.4 specification. ZigBee v1.1 will take advantage of the 802.15.4b set of revisions which were specifically commissioned to clarify ambiguities within the 802.15.4-2003 specification. It is expected that the release of the 802.15.4b will coincide with the new release of the ZigBee (v1.1) specification.

The ZigBee Protocol Stack

The ZigBee Alliance has generated several profile specifications that afford the generic foundation upon which you can create ZigBee-specific applications. In a similar manner to Bluetooth wireless technology, ZigBee *profiles* prescribe core use cases or applications that utilize the ZigBee protocol stack. The core profiles extend to common functionality, that is, marketed for *home*, *commercial* and *plant* use, but uniquely the stack provides scalability in that developers can create their own profiles to suit their particular application. The application will fall into one of the basic profiles as defined in Table 12.2, which encourage interoperability between ZigBee-enabled devices, very similar to the Bluetooth strategy. More specifically, a ZigBee network may comprise several profile types, which collectively form the basis of a *distributed* application.

Table 12.2 *A number of stack profile identifiers that may be used within a payload to specifically identify the profile in operation*

Identifier	Profile
0 × 00	Network related
0 × 01	Home control
0 × 02	Commercial
0 × 03	Plant control

For example, a switch on one node will communicate with a light on another node, in turn, they collectively form a simple light switch (on/off) application. Additionally, the manufacturer of the switch may differ to that of the manufacturer of the light and, as such, the profiles assure us of successful interoperation. In creating your own profiles, you must inform the ZigBee Alliance who will issue you a profile identifier where the developer must further define the *device descriptions*, *cluster identifiers* and *service types*. The profiles for home, commercial and plant have already been defined along with their respective device descriptions, cluster identifiers and service types.

Understanding the application context

A device descriptor is used to describe the types of devices that a ZigBee-enabled device is capable of supporting in addition to defining specific data attributes, which may relate to input/output streams and how such data should be formatted. These specific attributes can be grouped into clusters which too have their own unique identifies. It is the characterization of these device descriptors and clusters which uniquely creates the behavior of a profile. The ability to communicate data between nodes is achieved using service types; the *Key Value Pair* (KVP) service is used to provide a basic command/control mechanism between nodes. The *Message* (MSG) service type is a little more dynamic in that it uses the underlying KVP service as the transport mechanism to transfer data between nodes, but the payload can be application-specific and left to the discretion of the developer.

The ZigBee protocol stack, as illustrated in Figure 12.4 comprises several layers, which conform to the OSI model as we illustrated earlier in Figure 12.3. The stack is an eclectic number of layers, which are provided by a number of suppliers. For example, the PHY and MAC layers are defined by IEEE 802.15.4, whereas the NWK layer, *Application Support Sub-layer* (APS), the *ZigBee Device Object* (ZDO) and Application

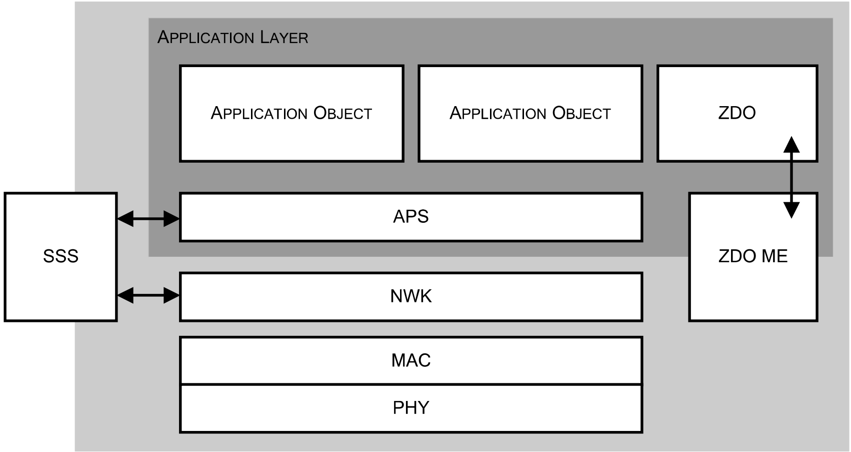


Figure 12.4 *The numerous layers that uniquely form the software building blocks of the ZigBee protocol stack.*

Framework are all provided by the ZigBee Alliance. The Application Objects are defined by the developer (or manufacturer).

ZigBee Device Objects

The ZDO has a significant role to play within the ZigBee protocol stack, in that it is responsible for defining roles and responsibilities for nodes (end-device applications) in addition to performing service and discovery procedures to learn of similarly-enabled devices in proximity and perform security, binding and network management. In addition to the above, the ZDO has responsibilities for housekeeping in the context of initializing the APS, the NWK and enforcing *security services specification* (SSS). The ZDO has a number of well-defined interfaces providing visibility to the application objects and interfaces through the ZDO management entity (ME) to and from the NWK layer and holistically supports the application framework. The notion of device and service discovery is very similar to that provided by Bluetooth wireless technology (see Chapter 11). The device discovery mechanisms afford the ZigBee-enabled device an opportunity to learn of other devices in proximity; the actual behavior in terms of applications support by another device is understood when applying service discovery. The binding procedure is a conceptual connection (or an *endpoint*) that is established between nodes that share the same or multiple applications (profiles) and are identified using the cluster identifiers; remember, these clusters contain attributes which let other devices know what to do. The multiple applications that a node supports will have multiple endpoints associated with it, which are logical connections that are bound (bind) when service and discovery procedures are performed.

Devices within the ZigBee network are bound (bind) when the nodes discover other like-minded nodes where these relationships that are formed are stored in a *binding table*. This table provides a quick look-up mechanism allowing nodes to quickly determine what is supported and what endpoint it is connected to. The binding procedure creates a relationship with ZigBee-enabled devices as peer-to-peer; (a) one-to-many (b) and many-to-one (c) as we illustrate in Figure 12.5. This topology affords ZigBee the diversity in the relationship in terms of multiple applications that a node might support.

The *application layer* (APL) offers a number of interfaces around the protocol stack to ensure successful communication occurs and in doing so the various layers that make-up the stack use a series of *Protocol Data Units* (PDUs). To achieve inter-communication between devices, there a number of service entities that transport data between the various layers of the protocol stack, namely the APS *Data Entity* (APSDE) achieving communication through the APSDE *Service Access Point* (APSDE-SAP). To manage and organize the discovered and bound (bind) ZigBee-enabled devices another service entity, APS *Management Entity* (APS-ME) is used along with its APSME *Service Access Point* (APSME-SAP). These managed objects are collated into a database, which is known as the APS *Information Base* (AIB). Likewise,

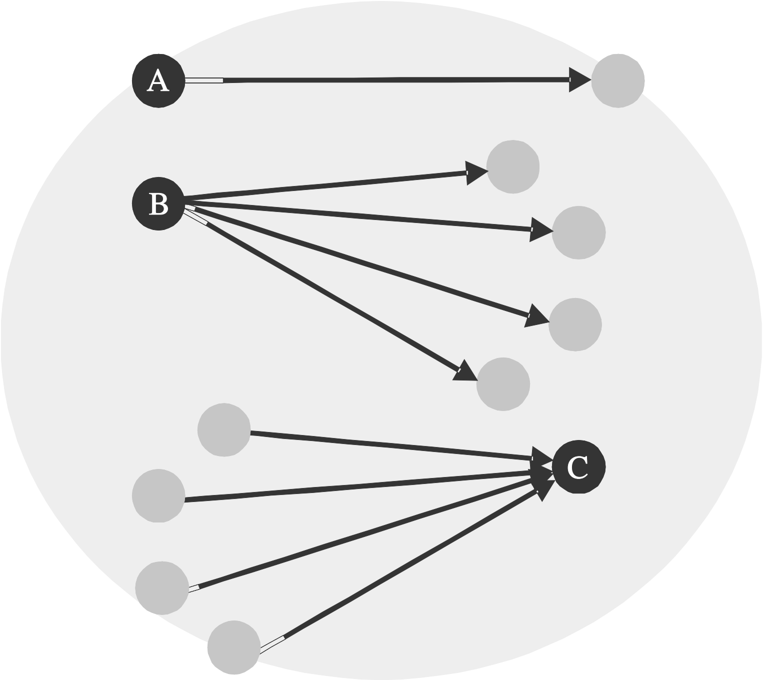


Figure 12.5 *The ZigBee relationships: one-to-many; many-to-one and peer-to-peer.*

at the NWK layer the application-specific data needs to move up and down the stack and there are service entities that ensure the NWK layer interfaces appropriately with the APL. In a similar manner to the APS, the NWK *layer data entity* (NLDE) supports a data service through a *service access point* (NLDE-SAP) and, of course, the ME integrally manages the intercommunication mechanism (NLME) and its associated service access point (NLME-SAP). Again, the whole data exchange is managed by a database and in this instance the managed objects are located in a *network information base* (NIB). More specifically, the NLDE transports application-specific PDUs (APDUs) between connected devices on the same network and provides services for the generation of a NWK layer PDU (referred to as an NPDU).

Conclusion

In light of the numerous technologies that are already competing with ZigBee it is hard to imagine that ZigBee will establish successful and fruitful market dominance. Likewise, its longevity is in doubt, as the initial pioneers seem to be moving on to fulfill other objectives. Although fatalistically, ZigBee has suffered a similar destination to that of Bluetooth, it has found a niche market, a unique application. Bluetooth has found a marriage between cell phones and headsets and ZigBee seems to have had moderate success within the lighting arena. It really is a niche and with ZigBee being implemented within this domain we can easily forget that it's there. We are reminded of that elusive killer application, but perhaps sadly, the only killing spree that will be endured here is the demise of ZigBee itself. It is hard to imagine where exactly ZigBee will fit in to the existing genre of wireless technologies, as we have already highlighted, other wireless technologies have succeeded. From a *Developing Practical Wireless Applications* perspective, it is really difficult to gauge where ZigBee will succeed: small toys and such, no-one really knows; lighting, home control, automation: still not sure, as everyone has had an opportunity at developing the smart home. Should we play devil's advocate here: does anyone care?

Summary

- The ZigBee Alliance ratified its standard wireless technology (v1.0) in December 2004 and made it public in June 2005.
- The Alliance is now finalizing v1.1, which takes advantage of the enhancements that were made to the original 802.15.4 specification.
- The new revision of the specification will be available at the end of 2006, start of 2007, but it is unclear as to who will be watching this damp squib.

- ZigBee seems to lack a basic feature set that so many other wireless technologies offer as a founding step forward.
- It seems that a significant number of the initial promoter companies are already abandoning ship; it really doesn't bode well for the future of ZigBee.
- The technology itself received an ambivalent response from manufacturers and the press alike, and its acceptance still remains somewhat muted.
- Many have argued that the need for the technology is futile, in the wake of other well-established technologies such as Bluetooth, Z-Wave and WiFi.
- Bluetooth Lite, a would-be derivative of the original specification, with its promised optimized *Media Access Controller* (MAC) should have naturally made ZigBee a regrettable mistake.
- The momentum behind Bluetooth Lite wavered and disinterest dominated the rigmarole of enduring yet another spat at defining a new technology.
- With more cost effective solutions for WiFi and a decrease in power consumption, WiFi at first glance appears to be a more obvious choice.
- Alas, WiFi is quite simply overkill for these types of applications such as toys, monitoring, control and so on; not just in terms of its data throughput, but moreover its application (software) base.
- There is a considerable overlap between ZigBee and Z-Wave (ZenSys).
- Zensys withdrew its support from the Alliance and essentially formed their own Z-Wave Alliance group.
- There isn't a great difference between the two technology solutions.
- Zensys has a clear advantage, as it has already established within the market a large consumer base of home control and automation products.
- ZigBee has yet to do this.
- Z-Wave is increasingly being seen as the de facto standard for wireless home control and automation solutions.
- The ZigBee Alliance has persevered and released their initial specification for the technology world to see and it continues to evolve the technology.
- ZigBee's inception is derived from a notion of simplicity.
- When we compare other standards-based wireless technologies, they tend to be larger, in software and hardware implementation terms, and consume more power.
- The foundation on which ZigBee is derived is a cost effective wireless model that the ZigBee Alliance hopes will become a de facto standard.
- ZigBee's topology, Z-Wave is essentially a simple one to understand.

- Numerous nodes are strategically deployed in an area, typically a home or office, where the radio coverage of one node overlaps an adjacent node.
- This enables the possibility of one reaching another even if they are thirty meters apart.
- In a relay style race the baton (data) is passed from one node to another until the destination node is reached.
- ZigBee's networking offers three topologies, namely the *star*, *mesh* and *tree*.
- The star implementation offers an application, a PAN context.
- A mesh implementation affords the application an end device, which may take the form of a FFD or a RFD.
- The tree topology is capable of extending the star topology.
- There are three device types within the ZigBee network: a coordinator, an end device and a router.
- The controller has the responsibility for creating and maintaining connections throughout the ZigBee network.
- ZigBee utilizes three ISM bands, namely 868MHz for Europe; 915MHz for the United States, and 2.4GHz for worldwide usage.
- ZigBee radios use DSSS this, in turn, affects how channels are allocated.
- The ZigBee network is very secure and uses an access control list only allowing known-nodes to enter the network.
- Authentication is assured by preventing devices impersonating other devices by using a common network key and establishing unique keys between device nodes.
- The 802.15.4 specification offers additional security features assuring users that their network is safe from intruders.
- ZigBee also uses the 128-bit AES algorithm, which discourages would-be eavesdroppers.
- A refresh timer is used to overcome replay attacks as a message has a certain window of time to reach a node.
- In an open standard such as ZigBee, interoperation is encouraged through the use of adopting a common platform upon which to develop wireless applications.
- ZigBee v1.1 will take advantage of the 802.15.4b set of revisions which were specifically commissioned to clarify ambiguities within the 802.15.4-2003 specification.
- It is expected that the release of the 802.15.4b will coincide with the new release of the ZigBee (v1.1) specification.
- The ZigBee Alliance has generated several profile specifications that afford the generic foundation upon which you can create ZigBee-specific applications.

- The core profiles extend to common functionality, that is, marketed for home, commercial and plant use.
- Uniquely the stack provides scalability in that developers can create their own profiles to suit their particular application based upon the core profiles.
- A ZigBee network may comprise several profile types, which collectively form the basis of a distributed application.
- In light of the numerous technologies that are already competing with ZigBee it is hard to imagine that ZigBee will establish successful and fruitful market dominance.
- Its longevity is in doubt, as the initial pioneers seem to be moving on to fulfill other objectives.
- ZigBee has suffered a similar destination to that of Bluetooth and found a niche market in lighting.
- It is hard to imagine where exactly ZigBee will fit in to the existing genre of wireless technologies.
- From a *Developing Practical Wireless Applications* perspective, it is really difficult to gauge where ZigBee will succeed.
- And does anyone care?

13

WiFi: Enabling True Ubiquitous Connectivity

This wireless technology probably doesn't need any introduction. Nonetheless, WiFi has truly captured a vast consumer-base and occupies a large number of homes and offices, and has also populated a number of street corners. The concept of making wireless was a really simple one. You have an 802.3 compatible *network interface card* (NIC), which plugs into a free *Peripheral Component Interconnect* (PCI) slot on your desktop computer; likewise, if you have a free PCMCIA slot on your notebook you would slot your NIC into here. You must surely remember the number of *Institute of Electrical and Electronics Engineers* (IEEE) 802.3 specifications? Of course, with the advent of wireless technology it does become easy to forget. The IEEE 802.3 defines the *Physical* (PHY) and *Medium Access Control* (MAC) layers for Ethernet; yes, good old Ethernet, which is still abundantly with us today and will be for some time. The concept to which we refer is wireless; take that NIC and transform into a *Wireless Network Interface Card* (WNIC). The IEEE 802.11, which is the working group that maintains and develops the WiFi technology, did just that. Incidentally, WiFi or *Wireless Fidelity*, is nowadays a brand name, trademarked and licensed by the WiFi Alliance (wi-fi.org), which undertakes the certification of the numerous 802.11 genre of products. More specifically, a manufacturer that has developed a technology that utilizes an 802.11 specification will undergo a certification program to ensure that the product complies with criteria that has been established by the WiFi Alliance. If the product satisfies the compliance criteria, then the product can display the WiFi Alliance logo. Nevertheless, we will use WiFi as a generic label to refer to any 802.11 specification. In Table 13.1 we illustrate the wealth of effort driving the future of WiFi and in this chapter we will undoubtedly refer to most of them.

The IEEE 802.11 specification defines the PHY and MAC layers for WiFi. In other words, 802.11 now replaces the 802.3 layers, in essence transforming the original NIC

Table 13.1 *The number of specifications that exist within the 802.11 family; at the time of writing this table was understood to be an up-to-date reference of the notorious alphabet soup. And, as for the letters that are missing, they are either available (disbanded) or the letters have been reserved*

	Description
802.11	The original standard developed in 1999. The specification supported 1Mbit/s and 2Mbit/s using the overcrowded 2.4GHz frequency.
802.11a	A 5GHz solution offering a data rate of up to 54Mbit/s, which was also offered in 1999.
802.11b	The most prolific and widely adopted specification, which comprised a number of amendments to the original specification. It was backward compatible with the original specification, but additionally offered 5.5Mbit/s and 11Mbit/s.
802.11c	A lesser known specification, but plays a crucial role within the WiFi genre of products as it enables wireless bridging between access points.
802.11d	Again a lesser known specification, which dominates much of the WiFi technology in use today as it provides harmonization within countries that are unable to use WiFi.
802.11e	An increasingly predominate specification that ensures your WiFi products sustain a good quality of service.
802.11g	Another prolific and widely adopted technology that offers backward compatibility with 802.11b. It emerged in 2003 offering data rates of up to 54Mbit/s.
802.11h	A standard that was specifically developed to overcome interference with the 802.11a specification, as there were issues with the 5GHz band interfering with satellite and other radio equipment.
802.11i	This specification primarily overcomes issues surrounding WiFi security and emerged circa 2004.
802.11j	A specification that was specifically drafted for the Japanese market to accommodate their rules regarding radio.
802.11k	With the prevalence of WiFi-enabled access points this specification was developed to enhance access point selection where multiple services are offered and is expected to be available in 2007.
802.11m	Intriguingly, this specification is a proposal by the 802.11 working group to ensure that all the specifications within the 802.11 family are maintained and are up-to-date; the IEEE began keeping their house in order back in 1999.
802.11n	Individually, this specification will keep other personal-area technologies on their toes, as it is set to compete with most wireless technologies that offer audio/video capability. It will be available in 2007 and is expected to be backward compatible with 802.11b/g/a offering a data throughput of up to an amazing 300Mbit/s.
802.11p	Another exciting specification that specifically targets the vehicle industry, not just your cars, but trains, airplanes and so on, and is expected to be published circa 2008.
802.11r	This specification complements 802.11k, as it alleviates issues surrounding roaming when presented with multiple services.

Table 13.1
(Continued)

	Description
802.11s	A specification that accommodates mesh networking. The standard is expected to be available in 2008.
802.11t	WiFi has populated numerous homes and offices and, as such, this specification ensures future reliability of the technology with its *Wireless Performance Prediction* (WPP) test method.
802.11u	WiFi increasingly finds itself integrated into a number of consumer electronic products and, as such, this specification affords a user the ability to connect to a network with some or limited services.
802.11v	This standard allows an administrator to manage and configure their networks and is very much still in its early stages of development.
802.11w	802.11i already offers increased security and authentication; this particular task group is working on amendments to the specification that will complement 802.11i and will protect management frames within the WiFi protocol.
802.11y	Another specification in its very early stages. 802.11y looks at the new available 3.65-3.7GHz bands and how they might offer broadband wireless services.

into WNIC. In Figure 13.1 we illustrate how both the 802.3 and 802.11 technologies can sit side-by-side whilst the rest of the stack above them remains oblivious to the transport medium; incidentally, in Figure 13.2 we illustrate the *Open System Interconnect* (OSI) model, which has been a common theme throughout *Developing Practical Wireless Applications*, as it remains pivotal when developing protocol stacks, and WiFi is no exception here.

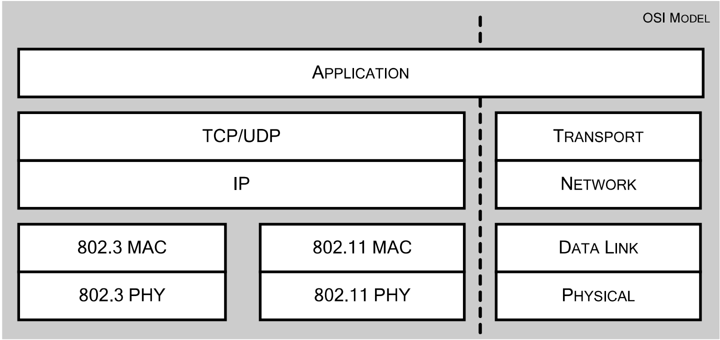


Figure 13.1 *On the left and right the 802.3 and 802.11 layers can sit adjacent to each other whilst the rest of the stack above them remains oblivious to the transport medium. Additionally, on the far right we have illustrated how this sits in parallel with the OSI Model.*

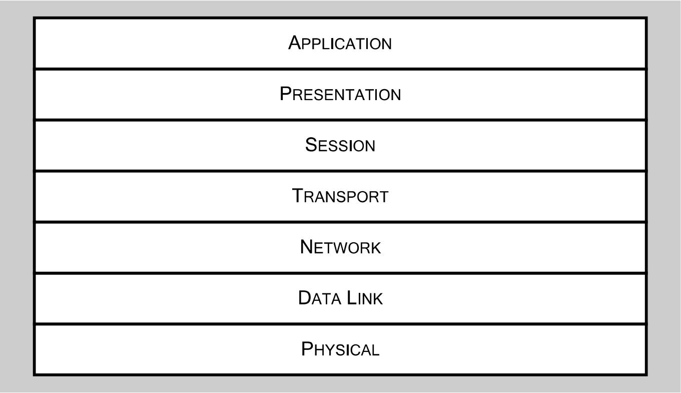


Figure 13.2 *The OSI model which, to a large extent, remains common to all wireless protocol stacks.*

Overcoming the Obvious

The sheer simplicity in transforming the PHY and MAC layers of the original NIC has now brought us the original 802.11 specification. But, not all is what it seems. A fixed networking environment, in fairness, was secure; hackers had to typically use another fixed network to attempt to gain access to your network infrastructure. In short, to achieve unauthorized access a hacker would more or less have to enter a property and physically connect the cable to a notebook – there are tried and trusted self-defense mechanisms keeping intruders out (we are referring to more than just security guards of course). Nowadays, wireless brings about a new breed of hacker; you may recall from Chapter 4, *Can we Confidently Rely on Wireless Communications?* when we compared a hacker to a tramp: someone who scavenges, but then went on to allege that they must have their hearts in the right place. Anyway, hackers have afforded us an insight into the vulnerabilities of the original 802.11 specification. As such, we have seen the IEEE vehemently strive to overcome these shortcomings and offer us *WiFi Protected Access* (WPA) which replaced the weaker *Wired Equivalent Privacy* (WEP).

The original introduction of WEP and its bias towards the RC4 algorithm has resulted in numerous attacks on WiFi. It seemed that WEP suffered from *key recovery attacks* where hackers made assumptions about the WEP key value based upon the value given in the unencrypted value which was prefixed to a ciphertext. Many individuals and companies alike have highlighted the ineffectiveness of the RC4 algorithm and with hindsight we have been afforded an opportunity to resolve the shortcomings efficiently. WPA (and WPA2) soon emerged after the weaknesses were identified with WEP. WPA became ratified by the IEEE in 2004 and WPA2 is the certified 802.11i specification. WPA offers us several new key enhancements, namely the *Temporal Key Integrity Protocol* (TKIP), the *802.1X User Authentication* and *Extensible Authentication Protocol* (EAP) which now, in combination, afford consumers greater encryption and authentication schemes. It was fortunate that the IEEE and the WiFi Alliance had such foresight, as implementing WPA2 into the home or office is a matter of upgrading to the latest software revision; albeit an inconvenience, it still sustains a life in a technology that has already commanded a strong market share as well as rewarding its dedicated consumers (if you wish to learn more about the specifics of WEP and WPA, then refer back to Chapter 4).

There's Something about WiFi

It's true: there is something about WiFi. What is it about WiFi that motivates and encourages spontaneous thinking which, incidentally, has *always* unconditionally been aptly suited to the conceived application, and needless to say, will undoubtedly continue to cause synaptic triggering within the deepest crevasses of our minds? Perhaps it's because it worked (more or less) from day one, with the exception of some security weaknesses. It was void of a time where there wasn't much hype about wireless technology (you only have to look at Bluetooth and more so, ZigBee to really put it into context). It is almost like we've never been without it. We can liken it to that of a cellular phone: it has always been there providing us a transparent service. And, in a similar manner, the majority of ordinary consumers are already aware of what it does and they know how to use it. Consumers today are still struggling to understand the basics of Bluetooth wireless technology (see Chapter 11, *Bluetooth: A Cable Replacement Technology*). Alas, WiFi is not completely without its dirty fingers after eating the chocolate cookies, as it seems that some consumers are a little frustrated when it comes to setting up their home equipment.

WiFi Protected Setup

In a move almost as fast as a synaptic nerve, the WiFi Alliance have offered us *WiFi Protected Setup*; an initiative that aims to simplify the configuration of WiFi equipment within the home and can also be extended to other consumer electronic devices. Although, if we refer to Chapter 14, *Near Field Communications: The Smart Choice for Enabling Connectivity*, we offer a more intelligent means of connectivity through *Near Field Communications* (NFC); this may have provided us a more transparent alternative. The premise of a more simplified mechanism for connectivity is based upon the consumer's *intent* to connect. For example, a WiFi *Access Point* (AP) in an airport is made available to the commuter who would simply approach the access point with his/her *Personal Digital Assistant* (PDA) or notebook notifying the WiFi access point that this device intends to connect to it. With sheer simplicity your wireless device has its default settings enabled. Nevertheless, the WiFi Protected Setup initiative is a valuable directive that will see yet more consumers embracing the technology with open wallets. The WiFi Alliance will adopt its ease-of-use strategy within the certification program and they will expect to start certifying products early in 2007.

WiFi Multimedia Power Save

In a mindset to dominate every conceivable consumer electronic product, the Alliance continually stays one step ahead of the market. In another initiative launched in December 2005, the *WiFi Multimedia* (WMM) Power Save certification program encourages manufacturers to reduce their power consumption by utilizing a more efficient data transmission scheme (as prescribed by the Alliance), in addition to tailoring the technology towards audio/video-specific capability. The data transmission scheme relies on the ability to send large data payloads in the shortest amount of time possible in an attempt to induce the WiFi hardware to sleep; in other words, the longer it stays asleep, the less activity, in turn, increasing battery life. Moreover, improved quality of service is assured with latency-dependent applications, such as audio and video, as traffic can be prioritized depending on the type of application being used. The WMM Power Save takes advantage of the existing power save features inherent within the original 802.11 specification, as well as taking advantage of several new features that have been introduced with the 802.11e specification. It is evident today that with new emerging cellular products, WiFi has increasingly been integrated within the phone to provide a seamless and transparent data connection that theoretically moves from WiFi to *General Packet Radio Services* (GPRS) and vice-versa – all being subject to the availability of a satisfactory service. What's more, with an increasing popularity in applications supporting *Voice over Internet Protocol* (VoIP), *Voice over Wireless Local Area Network* (VoWAN) and *Voice over Wireless Fidelity* (VoWiFi) as a medium in which cheap telephone calls (to cellular and landline) can be made, we will inevitably witness new cellular phones emerging with WiFi integrated as standard – very much to the disappointment of network operators. Additionally, in time we may even witness the emergence of WiFi-only phones or perhaps a combination of WiFi and *Worldwide Interoperability for Microwave Access* (WiMAX)-enabled phones.

Comparing WiFi and WiMAX

WiMAX is worth an introduction here, as it is often and mistakenly synonymously used alongside WiFi. The IEEE ratified the 802.16 standard in December 2001.

The 802.16 working group proposed a standard that would enable global penetration for *broadband wireless access* (BWA). It is also often referred to as *Wireless Metropolitan Area Network* (WMAN) and has been coined as WiMAX by the WiMAX Forum (www.wimaxforum.org). In a similar naming convention to that of WiFi, WiMAX is a registered trademark and brand name used by the forum to collectively refer to the genre of specifications devised by the IEEE. The WiMAX forum undertakes the certification of 802.16 products where a manufacturer that has developed a technology surrounding the 802.11 specification will undergo a certification program to ensure that the product complies with criteria that has been established by the WiMAX Forum. If the product satisfies the compliance criteria, then the product can display the WiMAX logo. Nevertheless, we will use WiMAX as a generic label here.

Like 802.11, 802.16 has seen a number of amendments and extensions, and in 2005 it saw a new update, namely 802.16-2005 that is now commonly known as *Mobile* WiMAX. The IEEE are in the process of making improvements to the 2005 standard. WiMAX is a different technology to that of WiFi, but many argue and perceive them as complementary and not competing, as they resolve two different problems. The first distinction to be made is the context in which you would use WiMAX and WiFi. In our introduction, we discussed the transformation that was made to our original NIC. Our NIC provided a network service for a number of fixed computers in a local area; this is what we have come to understand as our *Local Area Network* (LAN). When we transformed our NIC into a wireless medium (WNIC), we ultimately were still providing a network service for our local area network, but it meant that the computer did not have to remain static, that is, in the same location. The IEEE have defined WiFi to service our *Wireless* LAN needs (WLAN).

The provision of a LAN or WLAN, for either a home or office, may service many computers and may provide Internet access for its users. The Internet is typically connected to the greater telephone network through a fixed infrastructure. The fixed infrastructure relies upon cabling reaching every home and office irrespective of the terrain. However, in some instances the difficulty and cost associated with deploying such a cabled infrastructure for some *last mile* environments may be served much more economically with WiMAX; in other words WiMAX provides the *Metropolitan Area Network* (MAN). You may recall from Chapter 3, *Comparing Wide-area and Personal-area Communications*, when we discussed the overlap of wide- and personal-area technologies where nowadays the distinction is increasingly becoming blurred. The implementation of WiMAX is shown in Figure 13.3. A *base station controller* (BSC) is connected to the fixed infrastructure where a number of services, such as the Internet and/or telephony can be wirelessly provided to the *base station*. The base station then transmits its service covering a radius of approximately 10km (approximately 6 miles). In Figure 13.4 we illustrate how one such implementation of WiMAX can

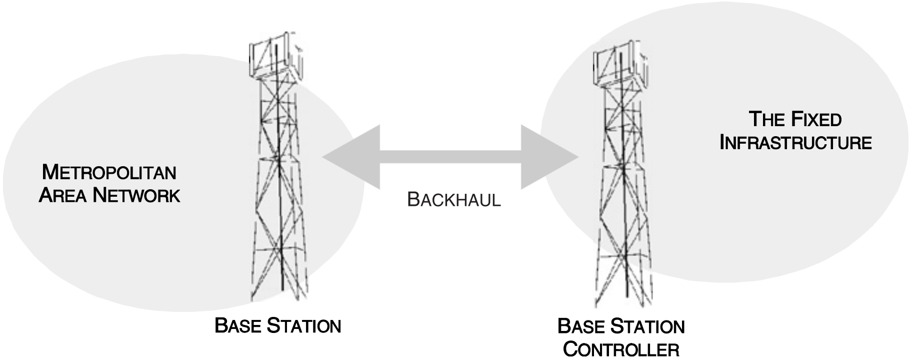
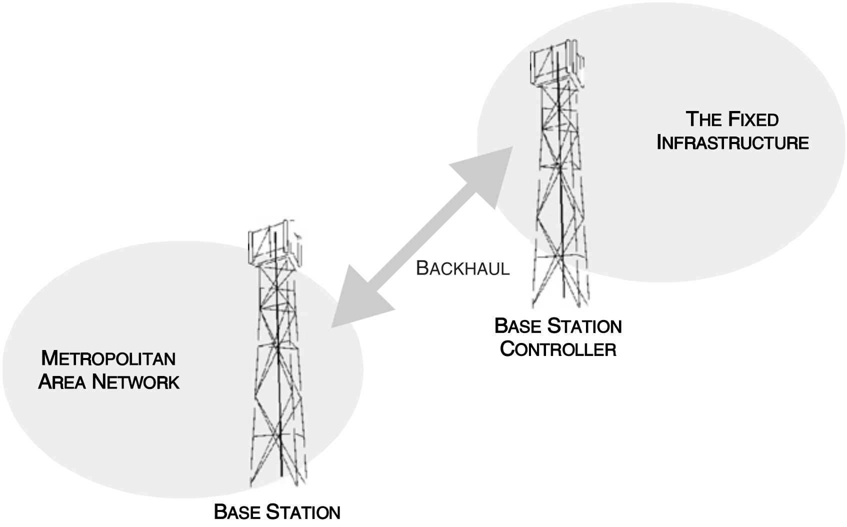


Figure 13.3 *The provision of a MAN is provided through a number of strategically placed base stations, which enable transceivers to relay services to a number of homes, office and mobile users.*

be used. A home or office may have an access point, similar to WiFi that, in turn, serves a local area network. Alternatively, in Figure 13.5 the WiMAX coverage essentially forms a *hotspot* that covers a radius of 10km for a number of mobile users.

In the latter context, it is expected that notebooks, cellular phones and other connectivity-orientated products will emerge onto the market with WiMAX silicon integrated as standard. For example, one such American manufacturer of silicon, which populates most computer-based systems with its processor technology, is

Figure 13.4 *The MAN may be delivered to an access point located at a central site in your home or office and, as such, it may provide access to the Internet for your LAN.*



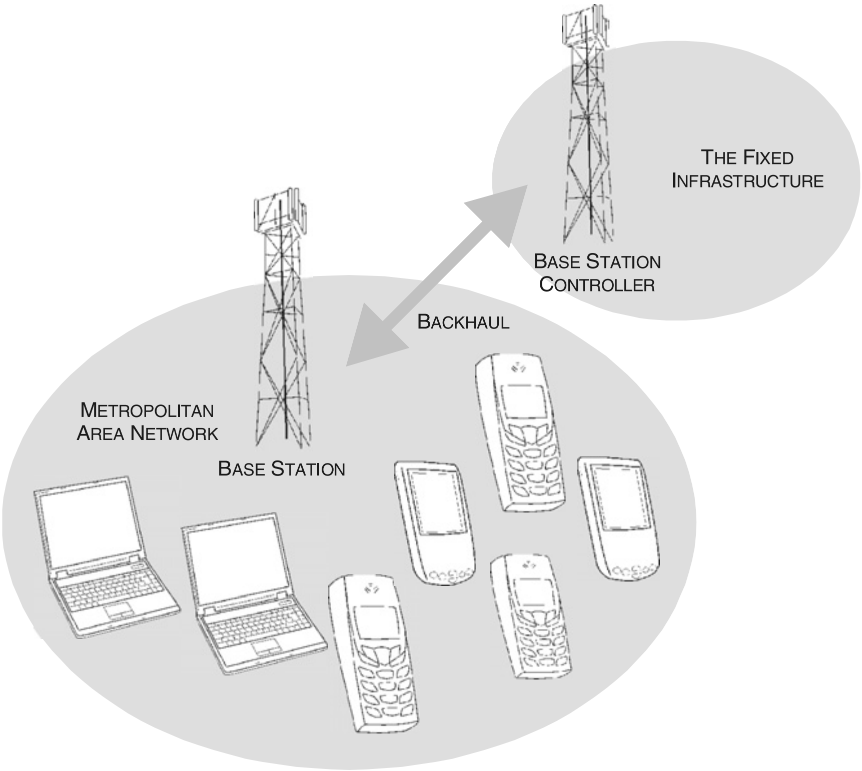


Figure 13.5 *The MAN may cover an area of 10km and, as such, if your notebook, cellular phone or PDA has WiMAX certified technology, then you will be able to access the larger fixed infrastructure for telephony and/or Internet connectivity.*

strongly advocating and has developed silicon ready for integration into the everyday PC. Naturally, this rollout coincides with an increasing deployment of WiMAX networks across the world; in particular, the United Kingdom has already provided a number of trial locations which have proven to be popular. You may have already guessed that 802.11 and 802.16 are two very different technologies in terms of what is expected at the PHY and MAC layers; new silicon has to be developed to accommodate this new genre of wireless medium. You may also be wondering what's the point, as WiFi provides a similar working model! Indeed, yet another wireless technology attempting to serve a consumer-base who may already be comfortable with WiFi.

One glaring fact is that WiMAX technology is superior to WiFi in that all the higher-level network management and administration features are in place from the initial onset and, as such, WiFi is still playing catch-up with its alphabet soup.

You may recall from our introduction that the 802.11v amendment is still being developed to offer management and configuration of WLANs. Nevertheless, this does not put a dent into WiFi's shiny amour as it has the superior advantage in that it has been around for many years and consumers have become accustomed to some of its idiosyncrasies. But, many would still argue, and the illustrations show, that WiFi and WiMAX serve two different functions. Let's put WiMAX into another context. WiMAX provides a service to mobile and cellular users that typically a WiFi network would not cover, although some trial installations have used a WiMAX-like connection for the *backhaul* (BSC to base stations) and implemented WiFi access points onto the base stations. Additionally, WiMAX has some compelling competition, as many cellular operators are deploying *High-speed Downlink Packet Access* (HSDPA), which competes with the usage scenario depicted by WiMAX. HSDPA is being widely deployed in Europe and is seen as a transitory technology between 3G and 4G, namely 3.5G. It seems that with an already existing cellular base and with cellular phones constantly being updated it would be perceived to be a more natural route to adopting a high-speed data link.

If we refer back to our discussion surrounding the popularity and emergence of VoIP, VoWiFi type applications and so on, it is not too difficult to conceive why WiFi- and WiMAX-only phones may become popular. With the deployment of HSDPA-enabled phones supporting an already established cellular network, the whole philosophy may become redundant. As such, cellular operators can breathe a sigh of relief as WiMAX will not necessarily hijack their current revenue stream, although it has been incredibly difficult for *Wireless Internet Service Providers* (WISPs) of WiFi technology to generate sufficient and sustainable revenue from users that connect to their service.

Generating Revenue from WiFi

It is clear that the sheer success of WiFi has been incredible and incalculable; well actually it probably is, as you only have to ask the manufacturers how much they have capitalized from offering WiFi products (and silicon) as a viable home and office solution. In addition to supplying WiFi access points you inevitably have to provide the computer client device (and its silicon) which, moreover, has been largely integrated within most computer systems. The ability to provide a product to a consumer or to a manufacturer for integration is reasonably straightforward and the revenue stream is somewhat predictable. However, many WISPs have unfortunately struggled to sustain a profitable wireless service through an access point or hotspot. From a consumer's perspective you may be placed in a context where you desperately need a wireless connection. One assumption here is that you are probably more than likely in a desperate situation to seek a cellular connection for voice as opposed to a data connection. In this situation a WiMAX network would be able to provide you with a cellular and data service or sustain a telephone call through VoWiMAX. Let us assume that you are eager to receive that all-important email. For example, you have traveled several hundred kilometers (miles) to provide a sales pitch and your potential client is refusing to physically connect you to their network (after all, they don't know you that well and it may provide you with an unfair advantage having such easy access to their network and its data). But, they duly inform you that there is a local WiFi service available in the area and they haven't chosen to implement wireless because they feel it's still insecure (why does this sound so familiar?). Anyway, you discover the number of wireless access points within range and you randomly select one. You proceed to make a connection and are presented with a web page informing you that you must log in and, if you're not previously registered then "click" here. The registration screen requests the usual information and, of course, that credit card number where typically you are charged $10 for an hour's connection. How much? Yes, that's right – and unknown to you at the time, must be a shock thing, you verbalize your thoughts loud enough for every one to hear. Nevertheless, you are impatient to receive that all-important email and concede to purchase what is a costly one-off payment. It may come as no surprise, when you pass through the registration screen where you are prompted with your login details, which quite honestly you never scribble down, as you only want the one email – that the service provider sends your login and password information to your registered email address (the one you used at registration) and your web browser doesn't save cookies because you are conscious of pop-ups, viruses and so on. But, the service provider has automatically logged you on to the Internet enabling you to retrieve your mail. Alas, it still hasn't arrived and you are reminded of time and that all-important sales pitch. In fairness to the wireless service provider, when you do return to your office, the registration email is duly in your inbox and you're able to use the login and password to access the wireless service any time you're next in the area.

In an unknown number of scenarios the presentation of the costly one-off payment tends to turn consumers away. Many carriers and network operators are shifting to a paradigm where the offer of a free service is made if you are already an existing subscriber to one of their products. For example, if you are supplied with a fixed telephone line service to your home or you are provided a cellular service, then in some business models the carrier or network operator enables you to freely connect to a wireless service (or through a wireless partnering scheme). In fact, it seems that you just can't give it away. In one such example, a major American aircraft manufacturer has withdrawn its intent to supply a wireless broadband service in its aircraft as there has been such disinterest from major airlines. It was envisaged that the service may have been provided to business users as a complementary service. On the other hand, a very popular low-cost Irish airline has secured plans to enable passengers to use their cellular phones and PDAs on their in-flight service. A roaming charge is made to use the in-flight service where voice and data call revenue is divided accordingly between the airline and carrier. The airline in question advertises and boasts a low-cost service, but will this be reflected in a low-cost voice and data service? But, more significantly, in light of the attempted terrorist attacks in London (Heathrow) where an alleged number of airplanes were targeted, new security restrictions now prohibit economy and business travelers from taking onboard any electronic equipment to include cellular phones, PDAs and notebooks. It is unknown whether or not these restrictions will become permanent and, as such, despite any well-architected satellite or cellular service, it may prove to be yet another empty revenue stream for wireless service providers. Although, it seems that the restrictions are limited to outbound services from London; other European airports seem to be somewhat more relaxed regarding items that may be taken onboard.

The WiFi Network Topology

The networking topology within a WiFi context doesn't greatly differ from that of any standard fixed LAN. In Figure 13.6, Figure 13.7, Figure 13.8, Figure 13.9 and Figure 13.10 we illustrate several typical implementations of a wireless-based network interconnected with multiple wireless networks and fixed infrastructure. However, a WiFi-specific network does come along with its own complications in addition to a new set of terminologies. In general, within a fixed LAN a notebook or desktop computer (or any other device that can be physically connected to the fixed environment) remains in a physical location and, as such, the destination can be addressed accordingly. Within a wireless environment a device (notebook, desktop computer and so on) is referred to as a *Station* (STA) where an STA may represent the message destination (or originator), as the destination does not necessarily represent the physical location. The distinction is made here to enable us to understand the flexibility afforded to us by wireless technology and the inherent complexity of addressing such devices. A further distinction should be made between *portable* and *mobile* devices. A portable device is a unit that can be used in a given location, but remains static within that location; for example, you may move a notebook from one room to another, but ultimately it remains fixed. A mobile device on the other hand, is a device that accesses the WiFi network whilst in motion; for example you may use a PDA to access the Internet and, as such, the device is moved around from room to room. Moreover, complexity is introduced with the time varying and asymmetric characteristics of propagation and, as such, it is not that simple to distinguish between a mobile and portable device. Nevertheless, they do provide us with dynamic topologies and with such dynamics, accompanied with the power constraints of such devices, we may experience a degree of unpredictability in sustaining a connection, as a device may move in and out of the WiFi service.

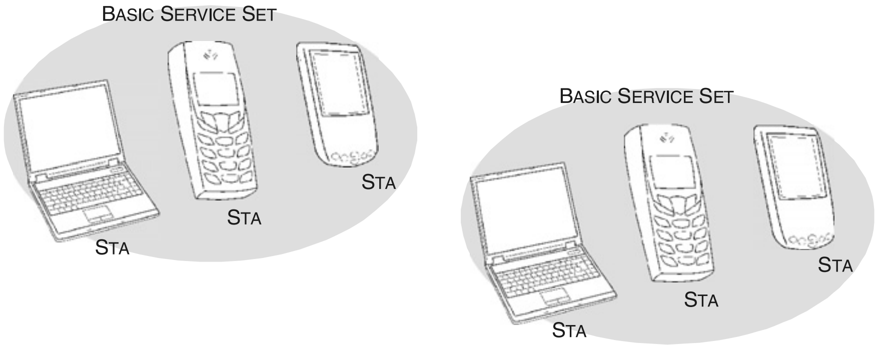


Figure 13.6 *The two basic service sets comprise a number of stations. While the stations remain in radio range, as denoted by the grey ellipses then the station has access to the wireless network.*

The independent and basic service set (BSS)

The *Basic Service Set* (BSS) is pivotal in a WiFi LAN and as shown in Figure 13.6 we can see that each of the BSSs have within their radio range (denoted by the shaded ellipses) a number of STA members. The STA itself provides a service, *Station Service* (SS) at the MAC layer, which includes authentication, confidentiality (formally privacy) and payload delivery; and whilst the STAs stay within radio range they remain part of the network and, as such, moving out of the shaded area as shown would preclude them from a wireless network service; we can describe the behavior of such a system as *dynamic* and an STA is deemed *associated* once it becomes a member of the infrastructure BSS. The association of an STA and BSS are dynamically created (that is, in or out of radio range) and, as such, are managed by the *Distribution System Service* (DSS); we will discuss this in more detail in a moment. More specifically, what is shown in Figure 13.6 are two *Independent Basic Service Sets* (IBSSs) where the STAs can informally join a network without the provision of an AP; this particular mode of operation is referred to as ad-hoc (network). An AP is also deemed to have very similar properties to an STA which, in turn, incidentally affords access to the DSS services through the *Distribution System* (DS).

Improved authentication and privacy

Following amendments to the original specification, 802.11i discusses changes that afford WiFi more effective security and confidentiality, and the DS and STA undertake specific procedures that take advantage of these new features. In particular a *Robust Security Network Association* (RSNA) procedure protects payloads and offers 802.1X

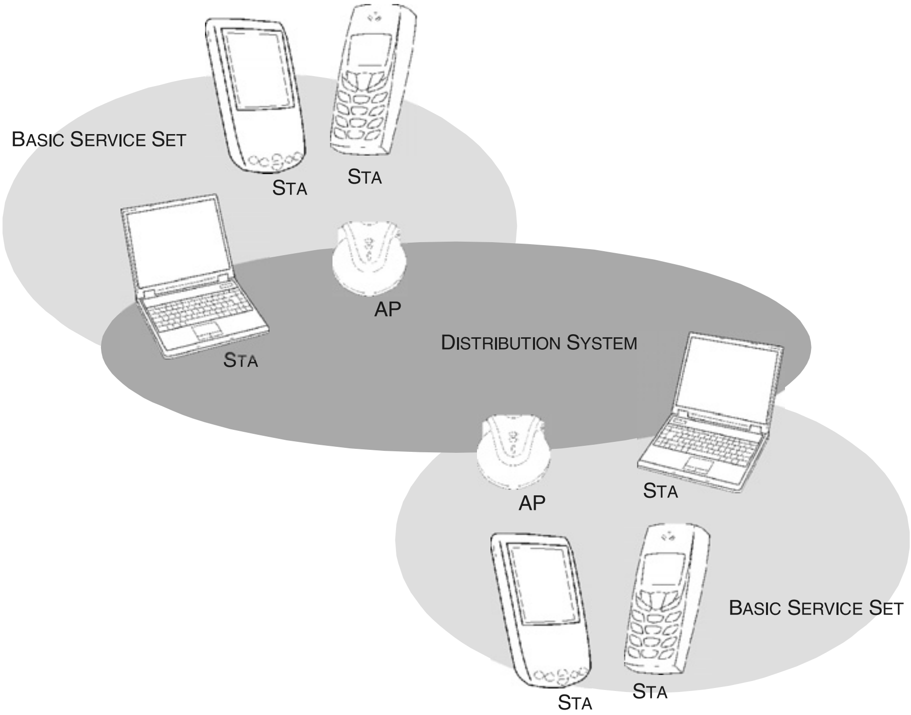


Figure 13.7 *A distribution system may connect a number of IBSSs together in addition to providing further services through an access point.*

authentication along with effective key management. You may also recall that we discussed WEP, WPA and WPA2 in greater detail in Chapter 4, *Can we Confidently Rely on Wireless Communication?* where the mechanics of such a new security ethos dispelled many of the perceived shortcomings of WiFi.

The RSNA mandates a basic set of security features, to include enhanced authentication for STAs and key management, along with WEP and 802.11 authentication. An *Authentication Server* (AS) is used as a sanity check mechanism and may authenticate the RSNA. Increased authentication and confidentiality is afforded by an 802.1X *Port Access Entity* (PAE), which is supported by all STAs. Likewise, an AP supports the PAE and put into context the AP PAE supports the role of *Authenticator* whilst the STA PAE honors the role of *Supplicant*; both roles implement the EAP.

Distributed System (DS)

A BSS has a limited coverage, due to the limited radio medium. Nonetheless, a WiFi LAN can be extended using a number of interconnecting BSSs. The interconnection is achieved through an AP and the architecture used to interconnect multiple BSSs is

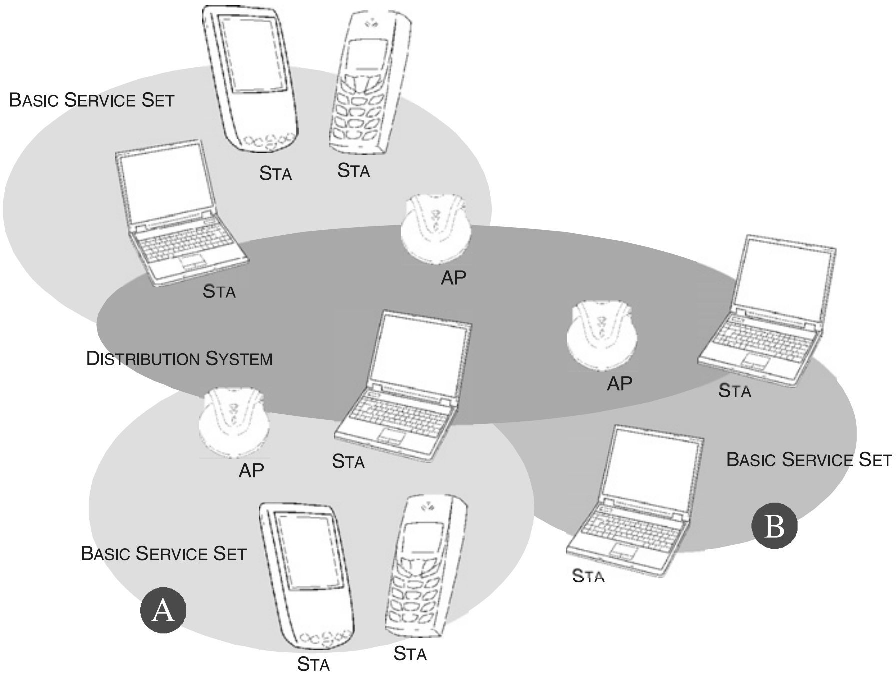


Figure 13.8 *BSS-A may partially overlap its radio coverage with BSS-B to provide continuity and a seamless connection for mobile users.*

a DS, as we discussed earlier and illustrate in Figure 13.7. The 802.11 specification proposes a logical separation between the wireless medium and the *Distribution System Medium* (DSM). In other words, the architecture that supports the wireless medium can be easily distinguished and separated. With such flexibility afforded by the PHY and MAC architecture they both can remain independent of any specific implementation of the DSM. What's more, mobile device support is achieved through logical addressing of an STA to multiple destinations. In Figure 13.8 we illustrate an implementation of several BSSs, but in particular you will notice that BSS-*A*'s radio coverage and BSS-*B*'s radio coverage are overlapped. Providing overlapping radio coverage assures mobile users' continuity with their WiFi connection; in turn, it supports a continuous uninterrupted service.

The Extended Service Set (ESS)

In Figure 13.9 we illustrate a scenario where the DS has access to a fixed LAN environment. The introduction of a *portal* continues the logical addressing theme, and in some instances an AP can offer both fixed LAN access and the services provided by a DS. A portal and an AP provide a holistic integration of the services available

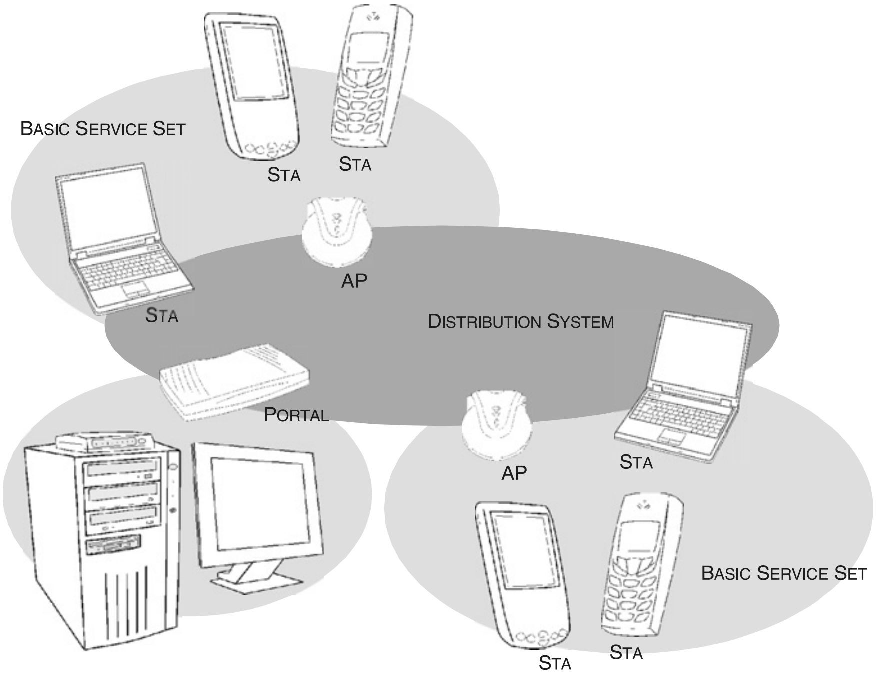


Figure 13.9 *A distribution system may connect a number of IBSSs together in addition to providing further services through a portal which may allow STAs to connect to the Internet.*

through, and supported by a DS. It is with the BSS and DS that a large area can be covered by a WiFi LAN, but the WiFi architecture also supports an *Extended Service Set* (ESS) network, where in some instances as we illustrated in Figure 13.7, Figure 13.8 and Figure 13.9 the actual logical assembly of all these devices appear as a single BSS to any STA, particularly at the MAC layer, as we illustrate in Figure 13.10.

Essentially, any station device, irrespective of its wired or wireless connectivity status, should appear to any other station or access point as a standard 802-LAN-type device. The importance of maintaining transparency at the MAC layer is significant in sustaining portability and mobility across multiple enabled networks. STAs that are part of a fixed LAN, that is, physically connected, can exchange LAN-specific traffic between LAN-like STAs. Likewise, any STA that is part of a WLAN can also exchange WLAN-specific traffic between WLAN-like STAs. However, merging STAs across a LAN and WLAN environment will ultimately compromise the implicit security of a LAN context. Although, confidentiality can be assured with the ability of the SS to ensure that WLAN traffic is protected and forms part of the confidentiality service maintained within the MAC layer. It is important to ensure that payloads are protected within any environment, as the default state is unprotected. It is also important to note that within an ESS context an AP may enforce a consistent security policy to

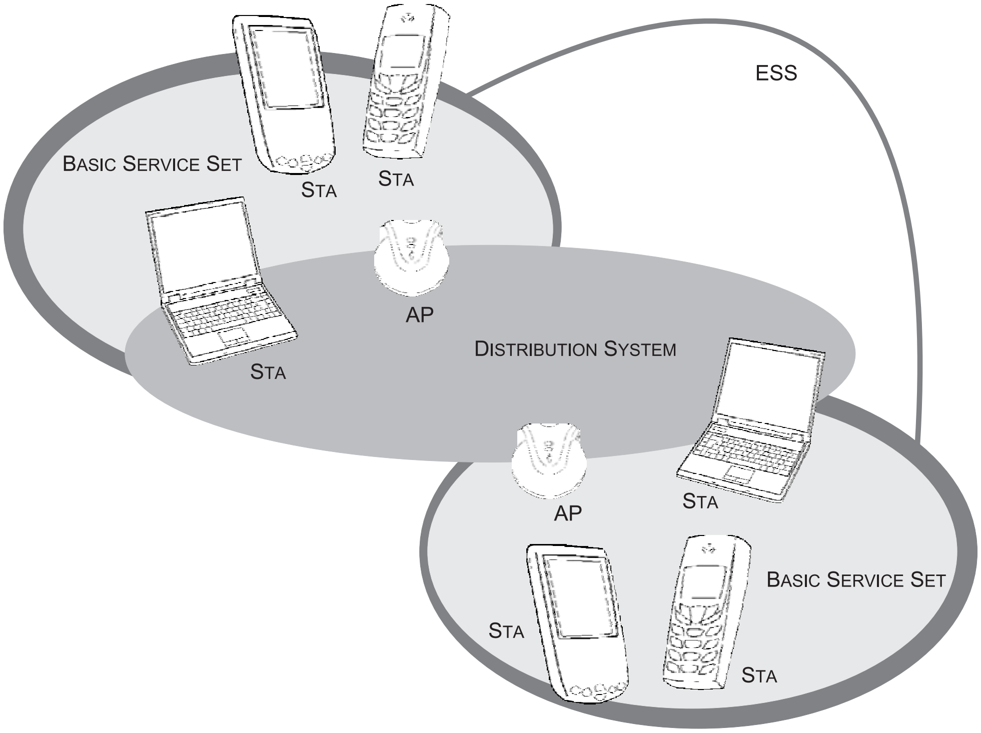


Figure 13.10 *The actual logical assembly of all these devices appear as a single BSS to any STA under an ESS context.*

all STAs. In the IBSS context, given the nature of the ad-hoc set-up of a WLAN, an STA can enforce its own security expectations.

The WiFi Story Begins with the Letter B

With an already established range of WiFi products and with the forthcoming 802.11n and 802.11p specifications where can we envisage the future of WiFi technology? In the following sections we define the architectures of the initial range of WiFi (802.11, 802.11b, 802.11g and 802.11a) products along with an educated prediction of what the advocates of WiFi would like to see the technology achieve.

802.11b, 802.11g and 802.11a: which came first? The original 802.11 specification can be perceived as a trial; a means by which the technology was first tested by consumers. Products emerged circa 1997 and, as an initial wireless introduction, it wasn't that well received, merely offering consumers 1Mbit/s and 2Mbit/s data throughput. It wasn't until 802.11b emerged in 1999 that we saw the uptake of what is now coined as WiFi becoming widely adopted. The beauty of 802.11b is that it offered backward compatibility for the small number of products that supported the original specification, but more importantly it clearly demonstrated the IEEE's intent and intuitive foresight. To coincide with the availability of 802.11b, 802.11a emerged in the same year. Incredibly, today you would struggle to locate an 802.11a product, as 802.11b still very much dominates the supermarket shelves. 802.11b uses the *Industrial, Scientific and Medical* (ISM) 2.4GHz band – you have undoubtedly become aware of the overcrowded use of this frequency with the relentless abuse of the unlicensed band presented within this book (WirelessUSB, Bluetooth and ZigBee are good examples). The technology offers a maximum data throughput of 11Mbit/s and degrades gracefully depending upon environmental circumstances down to 5.5Mbit/s, 2Mbit/s and 1Mbit/s where a more dependable service can be sustained in noisy surroundings. 802.11b formerly used the *High-rate Direct Sequence Spread Spectrum* (HR/DSSS) technique that was defined in the original 802.11 specification, but now uses the *Complementary Code Keying* (CCK) modulation scheme, which has now been widely adopted within 802.11b WLANs. Incidentally, additional research has been undertaken to determine the extensible possibilities with the 802.11b technology and, as such, with an external high-gain antenna, reports indicated that a range of up to 8km was achieved whilst in line-of-sight. It's not too inconceivable to deduce that the range is comparable with WiMAX. Incredibly, some manufacturers have taken the basic 802.11b specification and have absolved proprietary license with undue care and attention and provided a wireless throughput of up to 22Mbit/s. Naturally, these modifications are not recognized by the IEEE and consumers typically have to buy-in to the brand to achieve such data rates, which to be perfectly honest isn't such a bad thing, as you can be assured of interoperability and a common configuration interface between products. If a consumer has a mismatch of branded wireless devices and irrespective of unregulated modifications, the product would be assured to support 802.11b at 11Mbit/s as a maximum.

What became of 802.11a, as it is an obvious place to start? 802.11a uses the 5GHz band and presumably it seems a sensible approach to resolving the already overcrowded 2.4GHz usage and the apparent wealth of interference. Ironically, the 5GHz is subject to its own shortcomings, as the frequency is not robust enough to penetrate the most basic of obstacles, such as concrete, plastic, wood and so on. Similarly, it boasts a data rate of up to 54Mbit/s with an indoor range of 30m (100 feet) a range which is comparable to that of 802.11b. Comparing the HR/DSSS modulation scheme, the 802.11a on the other hand uses the *Orthogonal Frequency Division Multiplexing* (OFDM) modulation technique. However, 802.11b had an early product advantage, as 802.11a products only started to emerge in 2001 coupled with initial difficulties in sourcing of components and manufacturing. The deployment of 802.11b products was already immense at this time and it seemed as though consumers weren't going to be charmed into purchasing a technology that wasn't compatible with their initial investment. It seemed as though 802.11a couldn't get off its starting block.

In June 2003 we witnessed the introduction of 802.11g with a maximum data rate of 54Mbit/s and a range that was comparable with 802.11b and 802.11a. Additionally, it had the same robustness as exhibited by 802.11b and incredibly this technology offered backward compatibility with the existing consumer-base of 802.11b products, as it operated on the same 2.4GHz band. Uniquely, the 802.11g technology utilized the same modulation technique used by 802.11a, namely OFDM, and offered graceful degradation for data throughput, depending on environmental conditions; moreover, it was also capable of offering 802.11b support using CCK at 5.5Mbit/s and further degraded to 2Mbit/s and 1Mbit/s using the original HR/DSSS modulation scheme. With such flexibility it seemed an obvious choice for consumers and, to a greater extent, the technology press steered consumers in the right direction as opposed to "you must have this."

The WiFi Protocol Stack

The WiFi protocol stack is an eclectic piece of software which has been around for many years and silicon providers nowadays offer a varied number of drivers or software to interface with a number of microprocessors. When we compare the WiFi (or 802.11) protocol stack with Bluetooth and ZigBee it seems to be, at first glance, somewhat straightforward, as Bluetooth and ZigBee not only define their respective PHY and MAC layers, but a host of other layers that embody a wealth of responsibilities. You may recall from Chapter 12, *ZigBee: Untethered and Unlicensed*, and Chapter 15, *Ultra-Wideband: Introducing a New Short-Range Wireless Medium*, that both technologies have underlying PHY and MAC layers defined by the IEEE, namely 802.15.4 and 802.15.3a respectively. The emergence of WiFi evolved from the ability to replace a fixed connection (NIC-based) with a wireless medium (WNIC-based). In other words, the same protocols that exist above the NIC remain the same for WiFi, as shown in Figure 13.11.

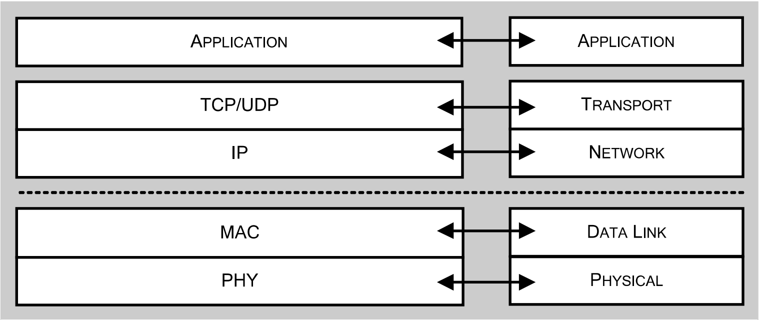


Figure 13.11 *The left side of the illustration forms our typical WiFi protocol stack architecture, which sits alongside the OSI model, as shown on the right.*

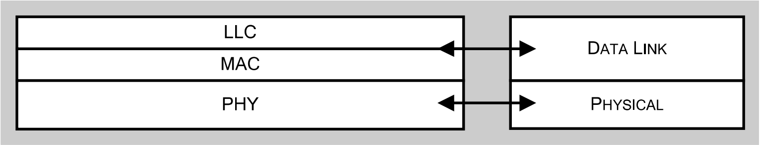


Figure 13.12 *The left side of the illustration depicts the PHY and the two sub-layers of our data link.*

The *Internet Protocol* (IP), *Transmission Control Protocol* (TCP) and *User Datagram Protocol* (UDP) sit on top of the 802.11 PHY and MAC layers. The application layer may form a number of applications to include a web browser (HTTP) or a mail client such as POP3 or IMAP and so on.

The MAC (Data Link) layer

In Figure 13.12 we illustrate the data link layer as two separate sub-layers: *Logical Link Control* (LLC) and MAC, but we will continue to refer to the data link layer as the MAC. If we compare this with Bluetooth, for example, the *Link Controller* (LC) or baseband layer is equivalent to our PHY layer and the *Link Manager* (LM) and *Logical Link Control and Adaptation Protocol* (L2CAP) form our MAC and LLC layers respectively. The division within the data link layer allows us to easily distinguish between the responsibilities of the upper- and lower-edge interfaces. In addition to these two sub-layers a governing *MAC Layer Management Entity* (MLME) is used to abstract and coordinate effort between the MAC sub-layers and the interface with PHY layer through a uniformed interface called a *Service Access Point* (SAP), as we illustrate in Figure 13.13.

The MAC layer performs higher-level functions within the OSI model and allows several physical layers to be positioned beneath it, allowing physical layer independence, as shown in Figure 13.14. It also manages access to the physical medium

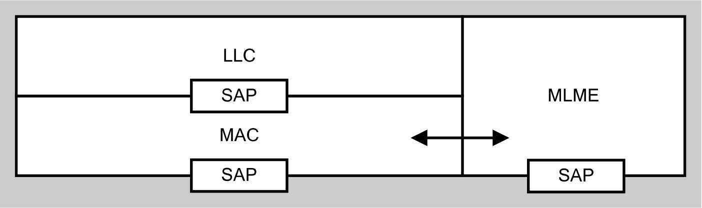


Figure 13.13 *The MAC and LLC sub-layers indicating the SAP interface with abstract support from the MLME.*

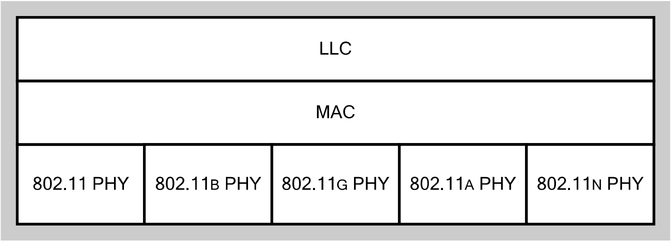
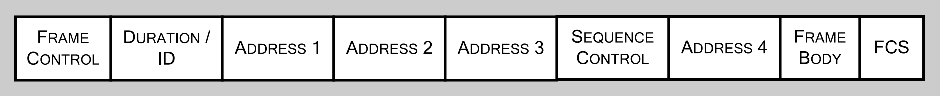


Figure 13.14 *The MAC layer bestows physical layer independence enabling a multiple number of radio mediums.*

and directs payloads accordingly. The MAC layer provides peer-to-peer connectivity in terms of directing payloads to the responding peer device. The MAC layer provides a number of services, to include *asynchronous data*, *security* and *MAC Service Data Units* (MSDU) ordering (a service used to re-order MSDUs if required).

The asynchronous data service provides peer-to-peer connectivity for MSDU, which uses the PHY medium to transport data to and from the peer device, as directed by the LLC sub-layer. The premise of payload delivery is made on a best effort basis where no guarantees are offered. Similarly, the transmission of broadcast and multicast MSDUs is done so at an impaired quality of service.

We have already touched upon some of the security mechanisms that 802.11 offers and, as such, the security service provides *confidentiality*, *authentication* and *access control*. The security service is supported by the authentication service, WEP, TKIP and *Counter Mode* (CTR) with *Cipher-block Chaining* (CBC)-*Message Authentication Code* (MAC) or CCMP procedures; the WEP algorithm is provided to support backward compatibility. You may recall from Chapter 4, *Can we Confidently Rely on Wireless Communication?* where we discussed issues surrounding *war-chalkers* and problems with eavesdroppers. WEP emerged as a solution to help protect data over the air interface by employing two strategies to ensure privacy and data integrity. In the former instance, cryptography (in particular, stream cipher RC4) is used to encrypt data over the air interface whilst data integrity is assured by using *Cyclic Redundancy Check* (CRC-32), a reliable checksum algorithm. WEP and its associated parameters used to encrypt data are inherently flawed. The introduction of WEP and its bias towards the RC4 algorithm resulted in numerous attacks. RSA Security, along with other academics/researchers, highlighted the ineffective strategy within the RC4 algorithm, namely the initial selection of the *Initialization Vector* (IV) value. WPA now supersedes WEP and addresses its shortcomings. As we just mentioned WEP is still supported to offer backward compatibility with the existing product-base. With several new key enhancements, namely TKIP, *802.1X User Authentication* and EAP the technology sustains greater encryption and authentication schemes. WPA became ratified by the IEEE in 2004 and WPA2 is the certified 802.11i specification.



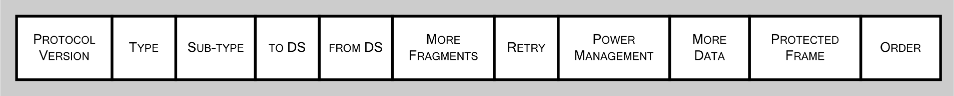
Frame Control	Duration / ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS

Figure 13.15 *The general MAC frame format.*

The MAC frame format

The MAC *Protocol Data Units* (MPDUs) is a sequence of fields that is transmitted down to the PHY layer, as shown in Figure 13.15 and it forms our MAC Frame. The MAC frame format comprises the *Frame Control* field, a *Duration/ID* field, *Address 1*, *Address 2* and *Address 3* fields, a *Sequence Control* field, *Address 4* field, a *Frame Body* field and a *Frame Check Sequence* (FCS) field.

The frame control field comprises a further set of fields, to include a *Protocol Version* field, *Type* and *Sub-type* fields, *to-* and *from-DS* fields, *More Fragments* field, a *Retry* field, a *More Data* field, a *Protected* field, which now replaces the *WEP Protected* field and an *Order* field, as shown in Figure 13.16. The protocol version is 2-bits in length and retains the current version of the standard in use. The type and sub-type fields are 2-bits and 4-bits in length respectively, and are used to determine the purpose of the frame, that is: *control*, *data* or *management*. The to- and from-DS fields are both 1-bit in length. The to-DS field is set to one to indicate frames that are destined for the DS whereas, the from-DS field is set to one to indicate frames leaving the DS. In the more fragment field, which is a 1-bit entity the bit is set to one to indicate that data and management type frames (as determined by the type and sub-type fields) have additional data to follow. The retry field is a 1-bit unit that is set to one to indicate that it is a retransmission of a previous frame. The power management field is also a 1-bit field and is used to indicate the STA mode in operation; a value of one denotes *power-save mode*, whereas a zero indicates that the STA will be in *active mode*. The more data field is used to indicate when an STA is in power-save mode that more data will follow. The protected frame field has been modified from the original specification, which just accommodated WEP operation. In the 802.11i specification the field



Protocol Version	Type	Sub-type	to DS	from DS	More Fragments	Retry	Power Management	More Data	Protected Frame	Order

Figure 13.16 *The Frame Control field.*

has been reflected to accommodate new additions to the standard, namely the TKIP and CCMP mechanisms, which we touched upon earlier. The 1-bit field, when set to one, is used to signify that data within the frame has been processed by a cryptographic encapsulation algorithm. Finally, the 1-bit order field is used to denote that MSDUs are being sent in a strict order.

In returning to our general MAC frame in Figure 13.15, the next field is the duration/ID field which is a 16-bit field and performs a dual task. The first task involves carrying an *Association Identifier* (AID) of the STA that transmitted a control type frame with power-save. In the second task the duration/ID carries a duration value for each frame type (control, data and management).

Basic service set identifier (BSSID)

The four address fields (Address 1, Address 2, Address 3 and Address 4) are used to denote the *Basic Service Set Identifier* (BSSID) comprising the *source* (SA), *destination* (DA), *transmitting station* (TA) and *receiving station* (RA) addresses; for each address 48-bits are used to uniquely distinguish each member of the BSS (STA, AP and so on). The formation and usage of these address types is shown in Figure 13.17 and is described in some detail in Table 13.2.

Service set identifier (SSID)

A BSSID is an address that is defined for each unique BSS and IBSS. In the former context a 48-bit address is used to uniquely identify a BSS, such as an AP; whereas, a 46-bit

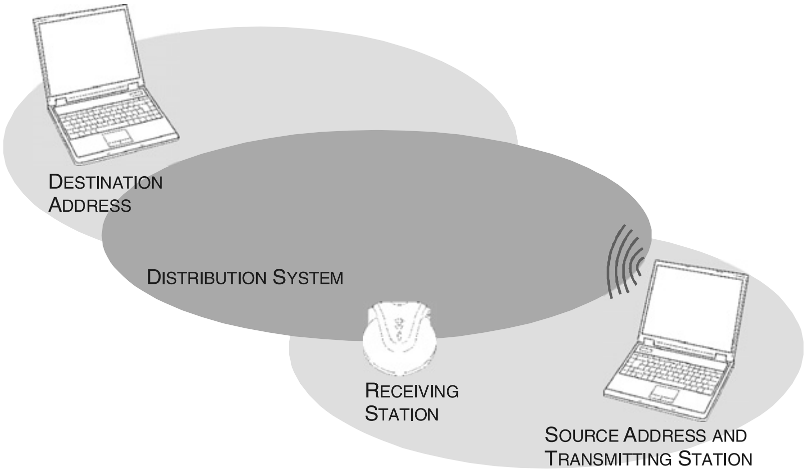


Figure 13.17 *The SA/TA transmits its MSDU for the DA, but the RA will relay the intended MSDU to the DA.*

Table 13.2 *A description of the various address types used within the MAC frame*

Address	Description
Source	A 48-bit address used to identify the originator of the MSDU.
Transmitting Station	A 48-bit address used to identify the STA that has transmitted the MPDU.
Receiving Station	A 48-bit address used to identify the intended recipient, such as a STA, of the MPDU.
Destination	A 48-bit address used to identify the final recipient of the MSDU.

random number is generated to uniquely identify an IBSS. A *Service Set Identifier* (SSID) is a unique field that is included within the MAC management frame and is used to identify a packet. The identifier is made up of thirty-two alphanumeric octets, which is typically identified by a user when connecting to an AP; some administrators choose to turn this identifier off in an ineffective attempt to hamper hackers.

The next field in the general MAC frame format is the sequence control field, which contains two further fields, as shown in Figure 13.18. The *Fragment Number* field is a 4-bit entity that identifies the number of the fragment of a MSDU. The 12-bit *Sequence Number* field represents the sequence reference of the MSDU which is assigned when an STA transmits its payload. The remaining two fields in our MAC frame format are the frame body and FCS fields. The FCS field is a 32-bit CRC, which is appended to the end of the MAC frame. Finally, the frame body is of variable length and essentially contains the message, which may be one of the frame types and sub-types, as we discussed earlier.

MAC architecture

The MAC sub-layer of an STA (for BSS and IBSS contexts), uses a *Distributed Coordination Function* (DCF) as a default procedure to determine if other STAs are transmitting before it transmits itself. The underlying mechanism used in the DCF procedure is the *Carrier Sense Multiple Access with Collision Avoidance* (CSMA/CA) mechanism. These procedures afford the MAC sub-layer to determine if the wireless

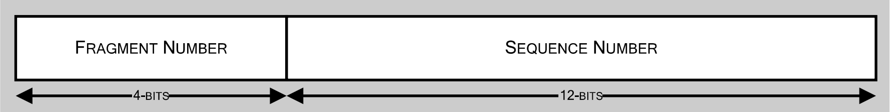


Figure 13.18 *The sequence control field comprises two further fields.*

medium is busy or idle; the specific action of determining this state is undertaken by the PHY layer, which passes it on to the MAC sub-layer. The MAC sub-layer also supports a virtual carrier-sense function, which is referred to as the *Network Allocation Vector* (NAV). The NAV affords the MAC sub-layer an educated guess at the traffic level based upon information it received from previous MSDUs. An optional mechanism is also used, namely a *Point Coordination Function* (PCF), which often resides on an AP. The AP employs a *Point Coordinator* (PC) to ascertain which STA can transmit, as it undertakes a polling mechanism to individually determine the status of each STA. The two mechanisms operate in parallel, as the two schemes alternate offering a *Connection-Free Period* (CFP) followed by a *Contention Period* (CP) in a BSS context.

The PHY layer

The PHY layer is responsible for establishing and terminating a physical connection with a peer device through the connected medium and preparing raw data to be transmitted over-the-air-interface. Likewise, the physical layer will also receive raw data from the air interface and prepare it for transmission to the MAC layer. In fact, the PHY layer is additionally broken down into two further sub-layers, namely the *Physical Medium Dependent* (PMD) sub-layer and the *Physical Layer Convergence Procedure* (PLCP) sub-layer, as we illustrate in Figure 13.19. In addition to these two sub-layers a governing *PHY Layer Management Entity* (PLME) is used to abstract and coordinate effort between the PHY sub-layers and the interface with the MAC layer through a uniformed interface called a service access point, as we illustrate in Figure 13.20. The SAP is a series of instructions or a primitive number of functions that afford simplistic exchange of communication between the MAC and PLCP.

The PLCP and PMD sub-layers

The PLCP sub-layer interacts with the data link (MAC) layer and has the responsibility to assemble PLCP *service data units* (PSDUs) or, in other words, they are MPDUs. Using this approach affords the PMD its independence from the MAC layer, as well

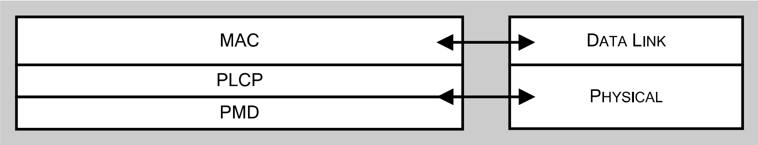


Figure 13.19 *The left side of the illustration depicts the MAC and the two sub-layers of our PHY.*

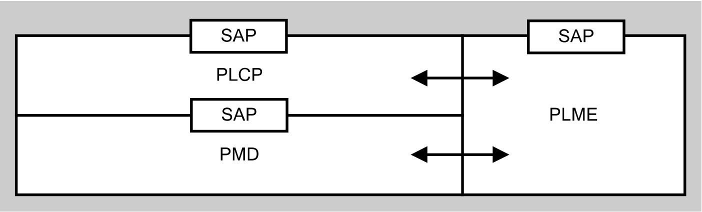
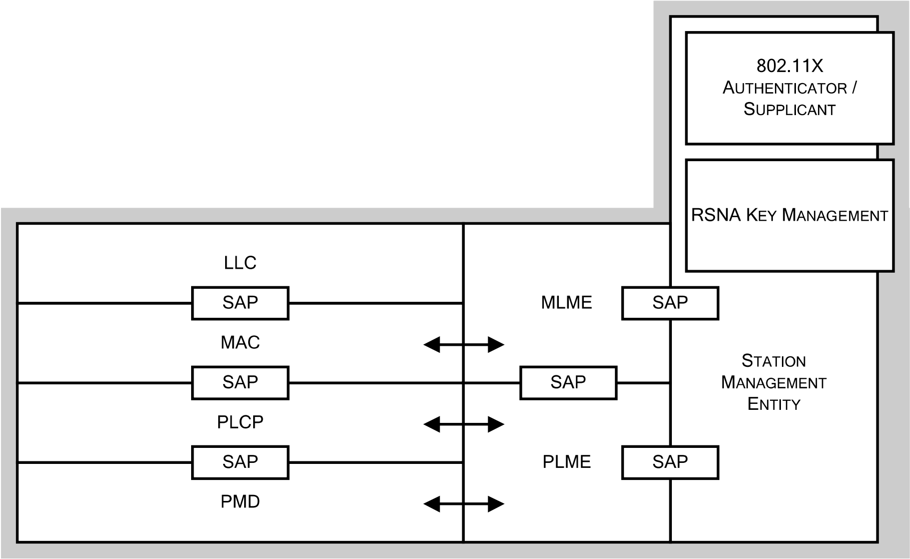


Figure 13.20 *The PLCP and PMD sub-layers indicating the SAP interface with the abstract support from the PLME.*

as, providing data that's in a suitable format for the PLCP. And conversely, the PLCP sub-layer will assemble payloads suitable for the MAC layer to understand.

The PLCP interacts with the PMD to enable PSDUs to be transmitted over-the-air-interface. The PMD itself has direct contact with the physical medium to facilitate in the communication of the connected medium; again, this is achieved through a SAP interface that supports primitive functions. Likewise, data received by the connected medium is formatted by the PMD to allow the PLCP to understand its content. In Figure 13.21 we illustrate the complete intercommunication of sub-layers for the PHY and data link layers. You should note that both the PLME and MLME work in conjunction with each other to support the communication between the MAC and PLCP sub-layers.

Figure 13.21 *The combination of the numerous entities that exist at the data link and physical layers. Each sub-layer has its own SAP interface with the respective sub-layer in addition to SAP interfaces with the relevant management entities.*



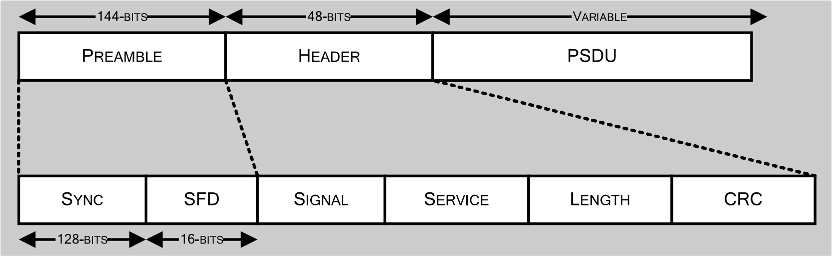


Figure 13.22 *The long PPDU comprises the PLCP preamble and header information, which is appended to the PSDU.*

802.11b PHY operation

As we discussed earlier, the 802.11b specification prescribes the high-rate extension for the DSSS method (HR/DSSS) with an 8-chip CCK, which affords the technology a maximum data rate of 11Mbit/s that degrades gracefully through 5.5Mbit/s, 2Mbit/s and 1Mbit/s, depending upon environmental and other factors.

During a transmit operation a PSDU is converted to *PHY Protocol Data Unit* (PPDU) by appending the PLCP preamble and header information. The format of a PLCP PPDU payload may differ in size, which is primarily due to the data rate being supported. The default payload comprises a *long* preamble and header, as shown in Figure 13.22; this would preclude the high-rate extensions (5.5Mbit/s and 11Mbit/s) where an optional short preamble and header are used, as shown in Figure 13.23.

The PLCP preamble contains the *synchronization* (Sync) and *start frame delimiter* (SFD) fields. The receiver uses the sync field as an early warning mechanism which notifies it of a new payload (using a series of ones and zeros) and the receiver should

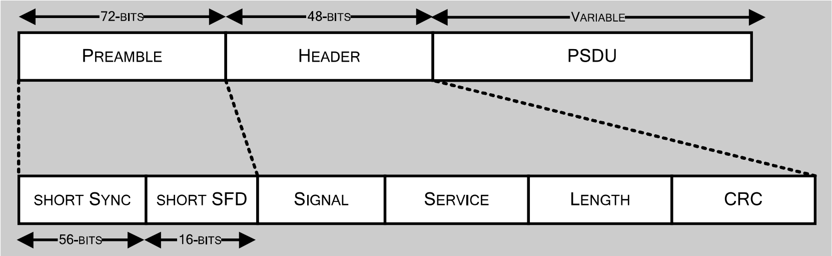


Figure 13.23 *The short PPDU comprises the PLCP preamble and header information, which is appended to the PSDU.*

Table 13.3 *The Signal field prescribes the specific data rate modulation that will be used for transmission and reception of the PPDUs*

Value	Rate
0 × 0A	1Mbit/s
0 × 14	2Mbit/s
0 × 37	5.5Mbit/s
0 × 6E	11Mbit/s

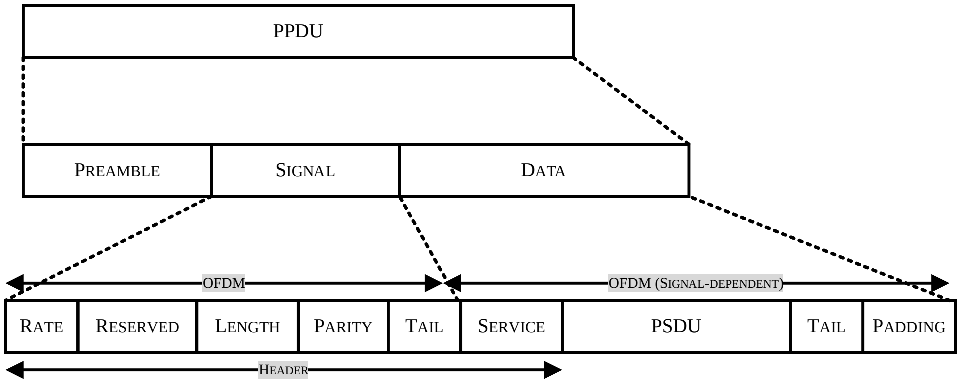
synchronize prior to receiving the SFD. The SFD is used to indicate that the start of a frame and the PHY parameters will follow. In the PLCP header an 8-bit *Signal* field denotes the data rate that will be used for the transmission and reception of the PPDU, as shown in Table 13.3. The values shown need to be multiplied by 100Kbit/s to reveal the true data rate value.

The *Service* field is an 8-bit value where only bits 2, 3 and 7 are used; bit 7 is used to supplement the *Length* field. Bit 3 is used to denote which modulation scheme is supported, namely CCK or *Packet Binary Convolutional Code* (PBCC); whereas, bit 2 is used to denote the transmit frequency and the symbol clocks are derived from the same oscillator and, as such, the PHY layer will set bit 2 to 1 (one) to indicate *locked clocks*. The *Length* field is an unsigned 16-bit integer that contains the number of microseconds that are required to transmit the PSDU. And finally, the CRC is used to protect the integrity of the signal *Service* and *Length* fields.

802.11g/a PHY operation

In this section we will discuss how the 802.11b specification differs from 802.11g/a. In our earlier section we discussed the 802.11g specification which prescribes the

Figure 13.24 *The ERP-OFDM PPDU differs from the 802.11b PPDU.*



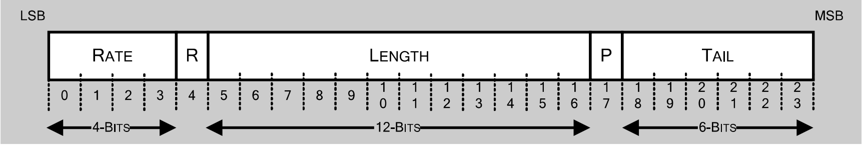


Figure 13.25 *The Signal field comprises a further five fields.*

extended rate of the HR/DSSS method. The 802.11g/a specifications discuss the *extended rate* of the *PHY* (ERP) layer and divulges compatibility with DSSS, CCK and PBCC modulations schemes which are supported by their respective data rates of 1, 2, 5.5 and 11Mbit/s. The ERP additionally increases the data rate to a maximum of 54Mbit/s and affords a graceful degradation through 48, 36, 24, 18, 12, 9, 6Mbit/s subject to environmental conditions. The data rates apply to both 802.11g and 802.11a in addition to the matching modulation scheme, namely OFDM.

Both 802.11g and 802.11a specifications share a similar PPDU format, as shown in Figure 13.24. The preamble and the header are appended to the PSDU, but the field make-up slightly differs, as shown. The ERP-OFDM PPDU, as illustrated, comprises a preamble, a *Signal* and a *Data* field. The *Signal* field comprises a further five fields, although the *Reserved* field will be used for future use and the *Parity* field will remain even for the bits zero to sixteen, as shown in Figure 13.25. Table 13.4 illustrates the possible combination of bit values that are used to determine the rate used for the physical interface (802.11g and 802.11a).

The *Length* field indicates the number of octets that need to be transmitted whilst the *Tail* field comprises 6-bits that are set to zero. If we refer back to Figure 13-24, we will continue to break down the respective fields. At the end of the *Tail* field (signal) we start to breakdown the units that comprise the *Data* field, which are the *Service*, PSDU, *Tail* and *Padding* fields.

Table 13.4 *The Rate field is used to denote the data rate used*

Value	Rate
1101	6Mbit/s
1111	9Mbit/s
0101	12Mbit/s
0111	18Mbit/s
1001	24Mbit/s
1011	36Mbit/s
0001	48Mbit/s
0011	54Mbit/s

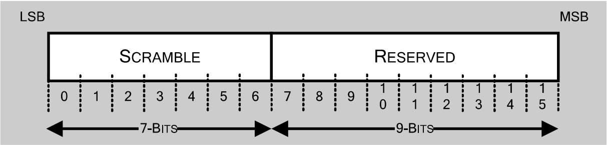


Figure 13.26 *The Service field comprises one additional field, Scramble.*

The *Service* field comprises one field, namely the *Scramble* field (bits zero to six), which is used to synchronize the descrambler in the receiver, as shown in Figure 13.26; the remaining bits within the field are reserved for future use and are all initialized to zero. The *Tail* field comprises six bits (all set to zero) which, in turn, are used to initialize the convolutional encoder. The final *Padding* field uses six bits, which are used to form the total number of bits that make-up the *Data* field as a multiple of the total coded bits in an OFDM symbol.

The PHY layer undertakes a number of operations to facilitate in the transmission and reception of data on the wireless medium. Typically, there is a transmit procedure, which is invoked when the MAC layer informs the PHY layer it has some data to transmit. Alongside the transmit procedure, an additional procedure is employed to determine if it is viable for the data to be transmitted. The *Carrier Sense* (CS) and *Clear Channel Assessment* (CCA) procedures are executed prior to the payload being sent to ensure that a channel is clear and that there is no incoming payload; this is very similar to the *Collision Detect* (CD) mechanism used with Ethernet data transmissions to ensure that there are no collisions on the physical medium. The receive procedure uses the same CS/CCA mechanisms to detect the preamble (sync field) followed by the SFD. You may recall that the sync field is used to notify the receiver of an incoming payload and, as such, must synchronize using the series of ones and zeros prior to receiving the SFD.

The Next Generation of WiFi

It is clear that WiFi has succeeded and dominated a market that is already filled with an overpopulated and under-used spectrum of wireless technologies. In an increasing need to stay several steps ahead of its competitors, such as *Ultra-wideband* (UWB) and Bluetooth (nowadays, we can perhaps discount Bluetooth as a competitor), the IEEE continues to evolve the technology. The most notable evolutionary step in the WiFi genre is 802.11n and second to that, the notion of which has been around for some time, is 802.11p. Both of these technologies are worthy of a paragraph or two, as they will inevitably launch a new range of wireless products in many years to come.

A new range of WiFi products 802.11n

In our initial introduction, we introduced the technology as potentially having a data rate of up to 300Mbit/s, but some reviews even dare to suggest that it may reach 600Mbit/s, although it's fair to say that this might be an exaggeration. However, some manufacturers have doubled the initial data throughput already offered by 802.11b, 802.11g and 802.11a with some proprietary alternatives. Nevertheless, it is envisaged that the 802.11n technology will capture a market that surrounds audio/video-centric applications. Furthermore, 802.11n will offer backward compatibility with 802.11b-, 802.11g- and 802.11a-enabled products.

The ability to offer backward compatibility is a fantastic marketing and business strategy, as many consumers have already invested in the existing range and, with an already estimated 250 million products in circulation, it would have been a difficult argument to persuade these advocates to start again. An ability to offer such support can be provided as the 802.11n uses OFDM modulation, which 802.11g and 802.11a already utilizes. The 802.11n solution offers three modes of operation, namely *Legacy*, *Mixed* and *Greenfield*. The legacy and mixed mode merely offer backward compatibility across a combination of 802.11b/g and 802.11a devices, but 802.11n must offer 5GHz to enable support for 802.11a legacy devices. It is expected that in the short to medium term 802.11n will operate in the mixed mode context, as the greenfield mode offers a pure 802.11n operation across all STAs and APs, which will naturally take advantage of the alleged bandwidth. Will consumers witness the predicted bandwidth as the 5GHz spectrum was filled with such shortcomings due to its inability to penetrate the most basic of objects? With the expected arrival of the 802.11n specification in 2008, many silicon providers have preempted the technology with their own derivative pre-802.11n solutions, which are unlikely to satisfy the criteria as defined by the WiFi Alliance. Incidentally, in an attempt to drive the awareness of this new generation of wireless technology, the WiFi Alliance have begun certifying pre-N solutions, which should alleviate initial unease with some early adopters (CNET News.com). Furthermore, some silicon vendors are wisely offering software upgrades to conform to the full specification when it is introduced; this does of course, allow consumers to confidently make that purchase now and enable them to take advantage of the new technology when it arrives.

Intelligent Transportation Systems (ITS)

The generation of ideas and technologies doesn't stop with 802.11n – 802.11p is also worth a mention here. It hasn't received a great deal of press, just some occasional anecdotal references (dailywireless.org). Nevertheless, the promise is to deliver an *Intelligent Transportation System* (ITS) operating in the 5.9GHz band. The 802.11p working group established the *Wireless Access in Vehicular Environment* (WAVE) offering a *Dedicated Short Range Communication* (DSRC) medium enabling a communications link between a vehicle and roadside equipment. It is envisaged that toll collection and vehicle safety will be the initial application-base, as well as intervehicle-communication.

Conclusion

If there is a single wireless technology that can proclaim to have changed the way we choose to live and work we have to attribute that trophy to WiFi. Other wannabes such as Bluetooth and/or UWB and ZigBee can only dream about capturing a significant percentage of the market. WiFi is evolving at such a fast pace not even UWB, WiFi's nearest competitor, will be able to keep up. As for the WiFi versus WiMAX contest there really isn't much to see, as WiMAX will have to battle it out with HSDPA. WiFi has made the steps forward it needs to be integrated into most consumer electronic products, but of course, it must avoid becoming complacent with its market share, although it's never advisable to be running and constantly looking over your shoulder. With a comfortable grounding and a well-defined future plan its future should be secure. The sun is still shining on WiFi and the wind is blowing gently in its hair – it feels good to be WiFi.

Summary

- WiFi has truly captured a vast consumer-base and occupies a large number of homes and offices.
- The concept of making wireless was a really simple one.
- Take that NIC and transform into a WNIC.
- WiFi is nowadays a brand name, trademarked and licensed by the WiFi Alliance.
- When a manufacturer develops a WiFi product it will undergo a certification program to ensure that the product complies with criteria that has been established by the WiFi Alliance.

- If the product satisfies the compliance criteria, then the product can display the WiFi Alliance logo.
- The IEEE 802.11 specification defines the PHY and MAC layers for WiFi.
- The sheer simplicity in renovating the PHY and MAC layers of the original NIC has now brought us the original 802.11 specification.
- A fixed networking environment was secure; hackers had to typically use another fixed network to attempt to gain access to your network infrastructure.
- Nowadays, wireless brings about a new breed of hacker.
- The original introduction of WEP and its bias towards the RC4 algorithm resulted in numerous attacks on WiFi.
- WPA (and WPA2) soon emerged after the weaknesses were identified with WEP.
- WPA became ratified by the IEEE in 2004 and WPA2 is the certified 802.11i specification.
- WPA offers us several new key enhancements, namely the TKIP, the 802.1X User Authentication and EAP.
- In a move that is almost as fast as a synaptic nerve, the WiFi Alliance have offered us WiFi Protected Setup.
- An initiative that aims to simplify the configuration of WiFi equipment within the home and office.
- The WiFi Protected Setup initiative is a valuable directive that will see yet more consumers embracing the technology with open wallets.
- The WiFi Alliance will adopt its ease-of-use strategy within the certification program and they will expect to start certifying products early 2007.
- In another initiative the Alliance launched the WMM Power Save certification program encouraging manufacturers to reduce their power consumption by utilizing a more efficient data transmission scheme.
- The data transmission scheme relies on the ability to send large data payloads in the shortest amount of time possible in an attempt to induce the WiFi hardware to sleep.
- 802.16 has seen a number of amendments and extensions, and in 2005 it saw a new update that is now commonly known as *Mobile* WiMAX.
- WiMAX is a different technology to that of WiFi, but many argue and perceive them as complementary and not competing, as they resolve two different problems.
- In some instances the difficulty and cost associated with deploying a cabled infrastructure for some last mile environments may be served much more economically with WiMAX.

- WiMAX provides the MAN.
- It is expected that notebooks, cellular phones and other connectivity-orientated products will emerge on to the market with WiMAX silicon integrated as standard.
- What's the point, as WiFi provides a similar working model?
- WiMAX technology is superior to WiFi in that all the higher-level network management and administration features are in place from the initial onset.
- This doesn't put a dent into WiFi's shiny armor as it has the superior advantage in that it has been around for many years and consumers have become accustomed to some of its idiosyncrasies.
- WiMAX provides a service to mobile and cellular users that typically a WiFi network would not cover.
- WiMAX has some compelling competition, as many cellular operators are deploying HSDPA.
- The ability to provide a product to a consumer or to a manufacturer for integration is reasonably straightforward and the revenue stream is somewhat predictable.
- Many WISPs have unfortunately struggled to sustain a profitable wireless service through an access point or hotspot.
- The networking topology within a WiFi context doesn't greatly differ from that of any standard fixed LAN.
- A fixed LAN, a notebook or desktop computer remains in a physical location and, as such, the destination can be addressed accordingly.
- Within a wireless environment a device is referred to as an STA representing the message destination (or originator).
- A portable device is a unit that can be used in a given location, but remains static within that location.
- A mobile device is a device that accesses the WiFi network whilst in motion.
- It is not that simple to distinguish between a mobile and portable device.
- The BSS is pivotal in a WiFi LAN.
- BSSs have within their radio range a number of STA members.
- The STA itself provides a SS at the MAC layer, which includes authentication, confidentiality and payload delivery.
- If an STA stays within radio range it remains part of the network.
- An STA is deemed *associated* once it becomes a member of the infrastructure BSS.
- The association of an STA and BSS are dynamically created.
- An STA joining/leaving in a BSS or IBSS network is referred to as ad hoc.

- An AP has very similar properties to an STA which, in turn, affords access to the DSS services through the DS.
- The DS and STA undertake specific procedures that take advantage of new features.
- A RSNA procedure protects payloads and offers 802.1X authentication along with effective key management.
- An AS is used as a sanity check mechanism and may authenticate the RSNA.
- Increased authentication and confidentiality is afforded by an 802.1X PAE.
- An AP supports the PAE and put into context the AP PAE supports the role of authenticator whilst the STA PAE honors the role of supplicant.
- The original 802.11 specification can be perceived as a trial.
- It was not until 802.11b emerged that we saw the uptake of what is now referred to as WiFi becoming widely adopted.
- To coincide with the availability of 802.11b, 802.11a emerged in the same year.
- You would struggle to locate an 802.11a product, as 802.11b still very much dominates the supermarket shelves.
- If there is a single wireless technology that we can proclaim to have changed the way we choose to live and work we have to attribute that trophy to WiFi.
- Other wannabes such as Bluetooth and/or UWB and ZigBee can only dream about capturing a significant percentage of the market.
- WiFi has made the steps forward it needs to be integrated into most consumer electronic products.
- It must avoid becoming complacent with its market share.

14

Near Field Communications: The Smart Choice for Enabling Connectivity

The concept of *Near Field Communications* (NFC) is based upon the premise of enabling through *proximity*. It's a simple theory but one shrouded with controversy, as we read of advertisers keen to acquire a sense of the long-term business plan for the technology. Many feel that it holds the key to a smarter, wirelessly-connected next generation of life-style enhancing products. It's certainly a sexier alternative to Bluetooth, being easier to use and brought to life by the slightest touch. You might even say that its market potential is foreplay to the eager consumer whose desire may be to rush discovery and introduction and simply get paired in an instance. NFC is not an entirely new technology – it just got smarter; it evolved from *Radio Frequency ID* (RFID) technology, which we can consider to be NFC's much older (and-all-around-nice-guy) brother. RFID has been around since the 1920s, but it formally emerged as various espionage tools during World War II and, of course, as a means of identifying airplanes as friend or foe.

What is RFID?

Most frequently, people use NFC and RFID interchangeably, but there are some subtle differences in terms of use cases, wireless medium and range. The premise of RFID is primarily to read information from a *tag* or *transponder* – a device that can be placed into a product or a person (yes, a person). The tag or transponder itself is an integrated circuit, which has attached a small antenna and can be placed into a number of materials. In fact, in 1998, a British cybernetics professor (Kevin Warwick) implanted a tag into his arm where he used it to control a number of devices to include light switches, doors and so on. The information stored on a tag will allow a *reader* or an *interrogator* to retrieve identification data pertaining to that product or person using radio waves. RFID has been used to track and trace products typically located in a warehouse and to monitor movement from a warehouse to a shop floor. A number of large supermarkets want to extend this a little further. As more and more supermarket chains increasingly compete on similar products, they would like to gain an insight and learn more about consumers' shopping behavior patterns. As such, they wish to associate our specific purchasing habits with loyalty cards and products purchased (CNETAsia). This data-mining exercise is well worn online but to be able to extend it to a wealth of daily options and choices merely through proximity monitoring would lead many of us to think twice before walking into that private members' club. This "big brother" type of scenario is clearly going to be hard to avoid, unless we choose not to participate in RFID/NFC's adoption, but many suspect that the volume of the technology's increasing benefits will outperform the cries of hysterical paranoia and eventually will turn the skeptics into advocates. Although, at this stage no one has objected to this claiming it's tantamount to "big brother," but it is still early days.

Operating frequencies

RFID is essentially a barcode replacement technology where reading information can be done automatically. Nowadays, with barcodes you have to use a device to scan whilst in light-of-sight, whereas an RFID reader conveys its data automatically using radio waves. The *Automatic Identification* (AutoID) system enables a unique monitoring system, ensuring products are tracked and logged when moved around a particular location such as a warehouse (goods in and out) for example. The tags are incredibly small, less than half a millimeter in size, and are certainly not obtrusive even with an antenna. They can be placed practically anywhere on the product and furthermore, unlike barcode readers where items have to be individually scanned, an RFID reader can more or less simultaneously read multiple tags. But, most uniquely, it has the ability to recycle the tag by updating it with new information allowing it to be used again and again. RFID offers three operating frequencies, namely *Low* (125kHz to 134kHz and 140kHz to 148.5kHz), *High* (13.56MHz) and *Ultra-high* (868MHz to 928MHz), but some global restrictions are imposed by the *Ultra-high Frequency* (UHF) due to the lack of a universal standard. The choice of frequency will be adapted to suit a particular application, for example the low frequency would be used to perform rudimentary tracking and access control. A high frequency option would be required if the environment was a little unforgiving such as metal structures in a warehouse and the radio range needed to be around two meters, but it would still support similar applications as that with low frequency. The UHF range accommodates similar applications to the above, but can prove problematic with metal structures and water, but typical RFID applications operate in the low and high ranges (RFIDJournal.com).

Active and passive tags

In addition to the availability of three operating frequencies, RFID can be categorized into two modes of operation: an RFID tag can be *Active* or *Passive*. The active tag is a battery powered device which, in turn, powers the onboard integrated circuit. It derives its own power from a battery which incidentally can sustain a life-span of up to ten years and has the ability to transmit a radio range of up to 100 meters. The active tag is a more robust alternative to the passive tag primarily because it has its own power source and, as such, it can be deployed in unfavorable environments where it will quite happily deliver. The passive tag, on the other hand, doesn't have its own power source and derives its power from the reader's radio waves, which seems to be sufficient to induce the integrated circuit to life. Indeed, a unit that has the ability to derive power from radio waves would surely have an unlimited life and its form factor would be incredibly small.

RFID technology is not restricted to identification, tracking or tracing; it too, like NFC, is used for payment systems, such as subway and vehicular access at tolls (see Figure 14.1), and key entry systems (very similar to the 802.11p standard, as we

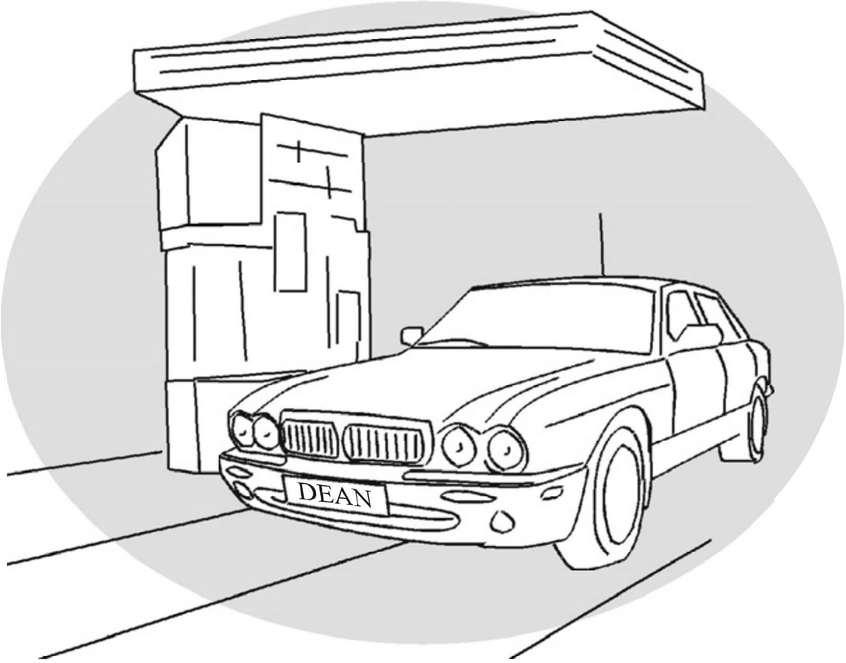


Figure 14.1
Many countries around the world are already using RFID technology to collect fares at toll booths.

discussed in Chapter 13, *WiFi: Enabling True Ubiquitous Connectivity*) and so on. RFID technology has evidentially been around for many decades, so why has NFC taken the limelight?

What is NFC?

Sony (www.sony.com) and Philips (www.philips.com) mutually developed NFC. The technology evolved from their contact-less or smartcard technology, namely *Felica* and *Mifare* which were respectively developed by Sony and Philips. The NFC standard was approved by the *European Computer Manufacturers Association* (EMCA), *International Organization for Standardization* (ISO) and the *International Electrotechnical Commission* (IEC) in late 2003. The standardization process affords true compatibility and interoperation of NFC-enabled devices and, as such, Nokia, Sony and Royal Philips Electronics launched the NFC Forum (www.nfc-forum.org) in March 2004 to direct the future adoption and deployment of NFC. Moreover, it seems that the forum wish to keep their cards close to their chest, as obtaining future use cases and software architecture documentation has been somewhat difficult to achieve. Nevertheless, they have made public several specifications, which are identified in Table 14.1.

NFC operates in the 13.56 MHz frequency range where the underlying protocol stack is based upon the various ISO, ECMA and ETSI standards. It is first and foremost an open specification technology, standardized for acceptance by the industry and ultimately to provide compatibility between devices of varying manufacturers. What's more, the standards specify the modulation schemes, coding, transfer speeds,

Table 14.1 *The number of public specifications made by the NFC Forum*

	Specification
1	*NFC Data Exchange Format* (NDEF) Technical Specification – this specifies a common data format for NFC Forum-compliant tags and devices.
2	*NFC Record Type Definition* (RTD) Technical Specification – this specifies standard record types used in messages between two NFC Forum-compliant devices and tags.
3	NFC Text RTD Technical Specification – this has been formatted for records containing plain text that can be read by NFC-enabled devices.
4	NFC URI RTD Technical Specification – for elements that refer to an Internet resource that can be read by NFC-enabled devices.

and frame format of the *Radio Frequency* (RF) interface of NFC devices, as well as initialization schemes and conditions required for data collision-control during initialization – for both passive and active NFC modes. Furthermore, the standards also define the transport protocol, including protocol activation and data exchange methods.

Sony's Felica, a wireless payment and ticketing system, uses NFC technology along with Philips' Mifare, which are both interoperable. Primarily, Felica is a wireless smartcard system that allows users to purchase shopping, cinema tickets and so on, using a cellular phone for example. Again, this whole concept isn't entirely new, but it's only now that we've seen it emerge into the public eye, presumably as a result of NFC. When consumers reach the check-out point, payment can be made by passing the cellular phone across a wireless smart card reader. The range of applications doesn't stop there either: wireless entry systems, such as *e-logging*, provide users the ability to enter buildings or to log on to a computer wirelessly. It is also envisaged that cellular phones will be used as a wireless entry system for your car and to start the engine.

NFC has an operating range of 5cm (1.97in) or 10cm (3.94in), although some manufacturers are extending this range for a host of other new applications, such as personal audio entertainment. You may want to refer to Chapter 9: *Aura Communications Technology: Creating the Personal Bubble*, where we discuss one specific example of how NFC-like has been used in a wireless stereo headset. RFID can exchange/read information up to three meters away, as compared with NFC's much shorter distance. It uses magnetic induction to transmit data from one device to another and inherently provides secure and reliable transactions. It's inherently secure because of the limited range and any malicious intent should be obvious. NFC-enabled devices can exchange data in either *active* or *passive* modes, very similar to RFID. In its passive mode, the *initiator*, or *master* device, starts the communication by providing the RF field which continues throughout the session. As previously discussed, it transmits data to another device, known as the NFC *Target* or *slave* device. The slave device transmits data back to the initiator without needing to generate a field by using a load modulation technique. The mechanism described can detect and connect with a target having the same connection and initialization procedure.

The fact that both the initiator and target devices can change roles where necessary makes passive mode operation an ideal power-saving and subsequently cost-effective method of wireless communication. In contrast, when in active mode, each device will need to generate its own RF field when data needs to be transmitted to another device to enable communication. This peer-to-peer communication allows for very fast connection between devices.

Our reasons to believe

The two founders of NFC, Sony and Philips, launched the technology with the intention of replicating the success they created through the introduction of audio compact disc recording in the 1980s. They immediately saw the market potential of a new wireless technology where the all too complicated passkey enabling of Bluetooth was removed and, instead, an immediate flow of data was created through the simplicity of *touch*. Having said that, the wireless range of NFC extends to 10cm, giving a whole new meaning to the phrase "mind the gap." The more recent addition of Nokia to the mix and the launch of the NFC Forum gave the group a forceful presence in the mobile sector which could be highly important in creating rapid adoption of the technology.

But will NFC drive another nail into Bluetooth's coffin? Some say yes, others no, but it is important to remember in all our excitement, that although the market potential for NFC is driven by its simplicity, it can never compete on the speed front. At 106, 212 and 424Kbit/s, NFC's data rate is, on average, closer to that of a 56Kbit/s modem than the 1Mbit/s or 54Mbit/s speeds of either Bluetooth or WiFi, so although cunningly simple to adopt within devices, it will never reach the finish line for the type of applications that Bluetooth and WiFi have managed to master. Perhaps its greatest strength is its enabling ability. We have already discussed the complicated pairing of devices in the Bluetooth arena. Now, if we consider the enabling benefits of NFC; demystifying the pairing process by removing it completely (in the minds of the users) and acting with "speed-dating" like efficiency in bringing the technology to life, we see that instead of an enemy, NFC could in fact be a useful ally in Bluetooth's future. Moreover, it could well be the partnership of the millennium if developers and promoters work together to ensure that they get the combination right and, with both Sony and Philips having a range of Bluetooth-enabled products within their market portfolio, they should be eager to get the marriage off to a good start.

Enabling intelligent connectivity

In adopting a common sense approach to wireless security, as we discussed in Chapter 4, *Can We Confidently Rely on Wireless Communication?* we clearly still assume that consumers will be comfortable with wireless terminology and usage. And, in an attempt to simplify the need to be familiar with such terminology perhaps we should consider a more intelligent approach towards enabling connectivity. The premise of a more simplified mechanism for connectivity is based upon the consumer's *intent* to connect, as we have already touched upon. If a consumer wishes to connect his/her Bluetooth-enabled cellular phone to a Bluetooth-enabled headset, then the consumer brings

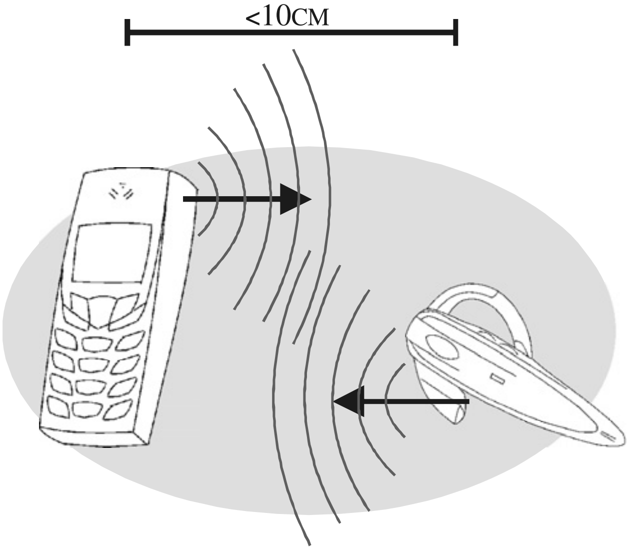


Figure 14.2
NFC has a short range of around 5 to 10cm and to enable connectivity the user must bring these devices within range.

together the two devices where they both transparently connect, as we illustrate in Figure 14.2. In this particular example, the authentication and configuration parameters remain oblivious to the consumer and in utilizing NFC over Bluetooth, the parameters are exchanged seamlessly between the two devices ensuring that the right devices are connected! Similarly, a WiFi access point in an airport can be made available to the commuter. The commuter would simply approach the access point with his/her PDA or notebook notifying the access point that this device intends to connect to it.

Application types

Developers are now in a position to take hold of the NFC promise and maximize its market potential within a wide range of products. It is evident that NFC promotes a different set of applications and to a large extent doesn't conflict too much with RFID's barcode replacement technology. It seems we can categorize NFC-based applications into three groups, namely, (i) *key based* – this category of application uses NFC as a key to *unlock* another service. For example, a so-called *smart poster* containing NFC tags, which promote a new product or service. Simply touching your cellular phone or PDA device against the embedded tag (or hotspot), would unlock the service and transmit marketing data to your cellular device in seconds; (ii) *peer-to-peer* applications. NFC is used to enable communication between two devices, such as a cellular phone, PDA, camera, printer, set top box and so on. An example of this would be a photograph taken with your mobile phone and then sent directly to your printer by simply touching it with the phone; and (iii) *pay and book* applications. Very similar to RFID, this area of NFC application is already growing. Many banks and cellular operators are waking up to the idea of offering payment and ticketing applications on phones and several credit card companies are currently trialing the technology in Europe. Additionally, plans are already underway to trial NFC technology within cellular phones to enable match passes within European football grounds. With NFC founders Philips being an official sponsor of FIFA (TalkNFC.com) this is a clever technology marketing alliance.

Conclusion

It is clear that NFC won't trounce on any other wireless technology; it will merely exemplify and support an ethos of simplicity, which is an unavoidable need to assure the success of any wireless technology. RFID is a barcode replacement technology and seems to be comfortable with its tag. NFC, on the other hand, does have some overlapping use cases with RFID, but it seems as though NFC will dominate a genre of consumer electronic products easing numerous use case scenarios such as connectivity, payment and entry. The technology roadmap is still unclear at this stage and, as we already mentioned, the NFC Forum wants to be sure of its future before proclaiming any outlandish applications.

Summary

- The concept of NFC is based upon the premise of enabling through proximity.
- RFID has been around for some time.
- Some people use NFC and RFID interchangeably, but there are some subtle differences.
- RFID reads information from a tag or transponder.
- A tag or transponder is an integrated circuit that has a small antenna.
- The information stored on a tag will allow a reader or an interrogator to retrieve data pertaining to that product or person using radio waves.
- RFID has been used to track and trace products typically located in a warehouse and to monitor its movement from a warehouse to a shop floor.
- RFID is essentially a barcode replacement technology and reading information can be done automatically.

- An RFID reader conveys its data automatically using radio waves.
- RFID tags can be incredibly small, less than half a millimeter in size, and are certainly not obtrusive even with an antenna.
- RFID tags can be recycled.
- RFID may use one of three operating frequencies: low (125kHz to 134kHz and 140kHz to 148.5kHz), high (13.56MHz) and Ultra-high (868MHz to 928MHz).
- The choice of frequency will be adapted to suit a particular application.
- An RFID tag can be active or passive.
- An active tag is a battery powered device which, in turn, powers the onboard integrated circuit.
- An active tag is more robust compared with the passive tag.
- A passive tag doesn't have its own power source and derives its power from the reader's radio waves.
- RFID technology is not restricted to identification, tracking or tracing.
- Like NFC, it is used for payment systems, such as subway and vehicular access.
- Sony and Philips developed NFC, which evolved from their contact-less or smartcard technology.
- The NFC standard was approved by EMCA, ISO and IEC in late 2003.
- Nokia, Sony and Royal Philips Electronics launched the NFC Forum in March 2004.
- NFC operates in the 13.56MHz frequency range where the underlying protocol stack is based upon the various standards.
- NFC has an operating range of 5cm or 10cm, although some manufacturers are extending this range for a host of other new applications.
- NFC uses magnetic induction to transmit data from one device to another and inherently provides secure and reliable transactions.
- NFC-enabled devices can exchange data in either active or passive modes.
- In passive mode an initiator, or *master* device, starts the communication by providing the RF field.
- It transmits data to a target or slave device.
- Both the initiator and target devices can change roles when necessary.
- It seems we can categorize NFC applications into three groups, namely, key based, peer-to-peer and pay and book applications.
- It is clear that NFC won't trounce on any other wireless technology.
- It will exemplify and support an ethos of simplicity.

15

Ultra-Wideband: Introducing a New Short-Range Wireless Medium

The proposition made by *Ultra-Wideband* (UWB) is what Bluetooth wireless technology should have been, but it seems as though Bluetooth has stolen some of UWB's thunder. You are undoubtedly aware of the alliance formed by the Bluetooth *Special Interest Group* (SIG) and UWB, more specifically the WiMedia Alliance. With a marriage of convenience, UWB didn't stand a chance. You only hear of such romantic stories in fairytales, but it seems as though the charming King has swept UWB off her feet, and we already know that Royal marriages are never that straightforward. In the newlywed's home, we may see the King struggle to carry the new bride over the threshold. Nevertheless, Bluetooth married into money and its future does look much wealthier as a result – Bluetooth can now confidently, with a helping hand from UWB's cash injection, reach a new level in its application-base. Without such support, we would have seen Bluetooth in a bankruptcy court and declaring to the judge "I spent it on establishing the right connections and women." In turn, Bluetooth would have ultimately become just a niche technology, serving only the cellular phone and headset. In a worst case scenario, Bluetooth would have become disbanded – having said that UWB/Bluetooth products are yet to emerge onto the market. It's not all that black and white though, as the marriage seems to be one of convenience – for Bluetooth at least.

WiMedia

You may recall our discussion in Chapter 11, *Bluetooth: A Cable Replacement Technology,* where we discussed the odd couple in question. Scouting around a number of sources attempting to retrieve a definitive answer to "What is WiMedia?" was at first difficult to ascertain. Although, according to the WiMedia Alliance (www.wimedia.org) website, WiMedia *is* UWB. The Alliance further defines five unique characteristics, namely *ultra-popular*, *ultra-friendly*, *ultra-trustworthy*, *ultra-smart* and *ultra-powerful*, which is primarily used to differentiate it from any other wireless technology. WiMedia is primarily targeted towards wireless multimedia-specific applications and it is abundantly clear that UWB can comfortably accommodate the genre of latency-specific applications that encompass audio/video and other home entertainment-based use cases, as we illustrate in Figure 15.1. An obvious reality of this technology is its commitment and support of Bluetooth, where it will provide a more supportive role in terms of data throughput. It is envisaged that a new Bluetooth core specification (possibly v3.0) will be drafted to accommodate Bluetooth over UWB. Yawn! Yet more pages to read and assimilate. It should be clear; UWB doesn't need Bluetooth. UWB can offer higher data rates and establish a more reliable data connection due to its multipath and wide bandwidth techniques. In many presentations of the UWB technology, many have argued that Bluetooth and UWB are competitors. Similarly, on these occasions, we may have become privy to numerous use cases illustrating how it would be possible for UWB to succeed where Bluetooth has failed.

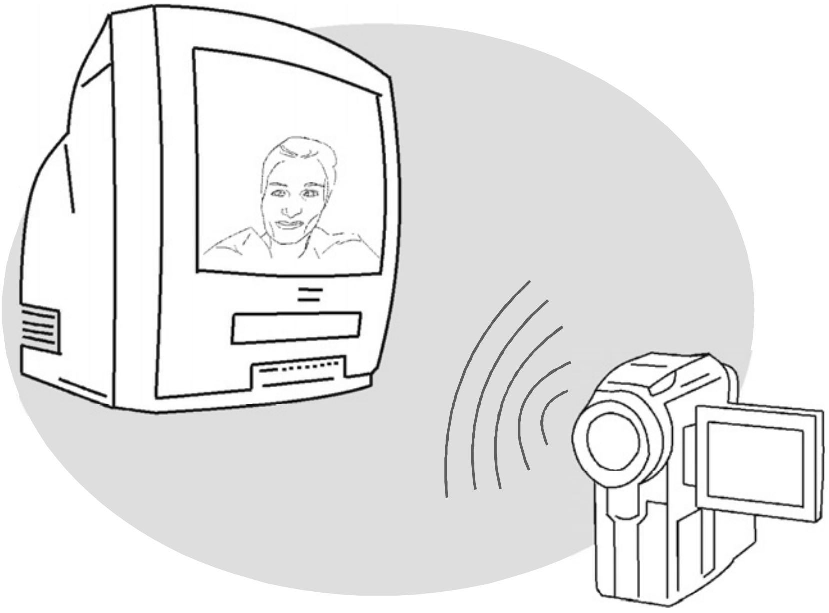


Figure 15.1 *With WiMedia consumers can enjoy direct streaming of audio and video from their cameras directly to their televisions.*

WirelessUSB

Bluetooth has taken several years to become visible to the consumer, albeit with a unique application (phone and headset). WiFi, on the other hand, is perceived to be ubiquitous. UWB (WiMedia) may achieve, or exceed, similar successes as WiFi has seen, possibly through a more appropriate marriage of USB and UWB, also known as *WirelessUSB* (WUSB). We can see that Bluetooth and its Royal-like status wooed WiMedia into thinking that they were a marriage made in heaven, but the true fairy-tale resides within the success of UWB and USB. The *Universal Serial Bus* (USB) has been around for almost as long as the PC and the simplicity afforded by such a technology has perpetuated the notion of connectivity as a basic task of plugging one end into another. As time has moved on, the Microsoft Windows *operating system* (OS), as well as other popular OSs have moved on too, making life much simpler for the everyday consumer. You simply plug in your USB-enabled device and the OS takes care of it all: the software installation and associated device drivers. Nonetheless, the advent of wireless was expected to ease the transition from cables to a cable-free environment. We are already familiar with a technology that has comfortably connected one device to another – and there's no getting it wrong as the connectors are transparent to any technophobe, despite the insistent pushing of the square connector into the round hole!

Bluetooth wireless technology was the first to boast the possibility of extending the USB ethos into a wireless medium and Cypress Semiconductors in its frustration was eager to demonstrate its WUSB solution using the 2.4GHz band. You may recall in Chapter 8, *Cypress Semiconductor: Introducing WirelessUSB*, we discussed Cypress's own flavor of WUSB in response to a frustrated market that was keen to take the next step. USB already serves a plethora of peripheral devices, such as a keyboard, mouse, joystick, printer, external hard drive or CDROM, broadband modem, and so on, as illustrated in Figure 15.2. The challenges presented to WirelessUSB to outshine the facets of an existing and well-established technology are certainly daunting. In fact, WirelessUSB doesn't really have to do that much to stand out, as the basic premise itself is the removal of the cable and so, from a consumer's perspective, the same flexibility and simplicity inherently exists. Indeed, the WiMedia Alliance have already partnered with the USB Forum (www.usb.org) to thrash out a way forward for a harmonious relationship.

Using near field communications as an enabler

Near Field Communications (NFC) would have been a more obvious choice as an alliance, as the technology lends itself well as an enabler. You may recall our discussion in Chapter 14, *Near Field Communications: The Smart Choice for Enabling Connectivity*,

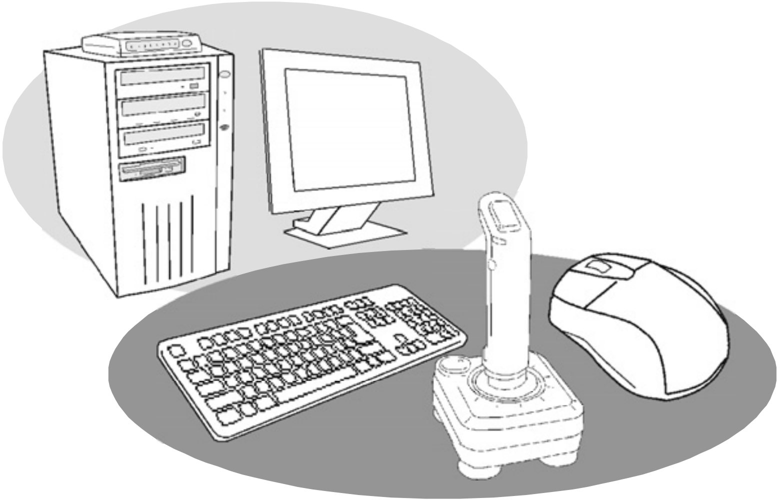


Figure 15.2 *WiMedia's WUSB can comfortably accommodate the plethora of consumer electronic devices with unquestionable ease.*

where we discussed how NFC would alleviate connection set-up and authentication with Bluetooth and WiFi products as shown in Figure 15.3. Since WiMedia intends to populate a host of consumer electronic products it should really avoid the necessity of discovery mechanisms and other such nonsense when establishing relationships with other suitably enabled products. This is not to say that authentication and encryption should be left void, but using the ability of NFC as a technology enabler would further ensure the simplicity consumers so desperately need.

Conflicting UWB standards

The importance of establishing a number of organizations whose responsibility it is to ensure the future direction of wireless technologies would be reliant upon their reading from the same page, or so you would assume. However, it seems that the WiMedia Alliance and the UWB Forum are singing from two different pages. The WiMedia Alliance has adopted the *Multiband Orthogonal Frequency Division Multiplexing* (MB-OFDM) version of UWB. The UWB Forum, on the other hand, has adopted the *Direct Sequence* (DS) version; you can already see this is just going to end in tears. This is evident as the Bluetooth SIG has expressed an interest to work closely with both groups; now we will surely hear rumors in the papers that the King is in bed with UWB's sister. Again, in light of Chapter 1, *Making Sense of Wireless Technology*, we do have to apply a sense of proportion and reality when developing technologies that are targeted to simplify many use cases. It is bewildering to read that there are two flavors of UWB, which will ultimately go head-to-head in a battle to dominate. However, Freescale and Motorola have both withdrawn their commitment from the UWB

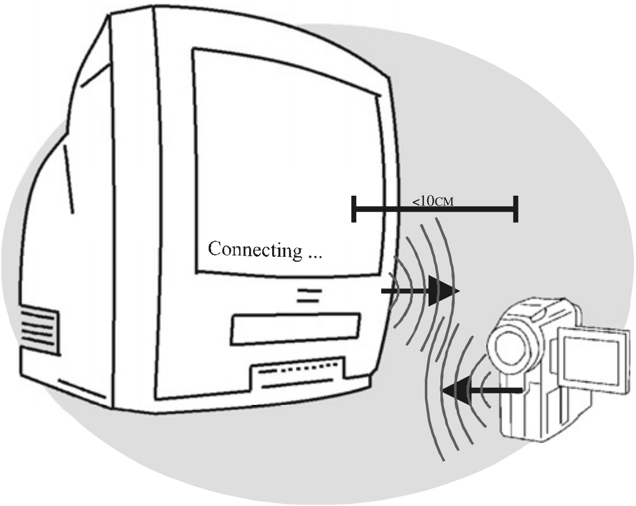


Figure 15.3 *Utilizing NFC as a technology enabler for WiMedia-based products will guarantee simplicity in many of the expected use cases, as envisioned by the Alliance.*

Forum (EETimes.com, October 2006). Freescale and Motorola, along with Pulse-Link founded the forum in 2004 and, as such, it must leave the remaining members (over one hundred or so) reeling. Naturally, the remaining members may be feeling vulnerable and uncertain about their future and, as such, the WiMedia Alliance should take an opportunity to grotesquely abuse its advantage.

Conclusion

UWB can stand on her own two feet and provide an effective and robust wireless technology that will embarrass Bluetooth. The simple truth is that WiMedia doesn't need Bluetooth; WiMedia can stand alone and deliver consistent and secure wireless technology branded as WirelessUSB. Bluetooth adds another level of complexity, which will ultimately confuse a consumer-base that is already struggling to keep up with the three letter acronyms. In the background we often muse with humor as consumers struggle to understand them. At least with USB and a 21st century transition to wireless wouldn't be a far stretch for an average Joe Blogg consumer to understand. WiMedia needs to keep a steady hand when launching the UWB flavored products, as it really can't afford any possible misunderstanding.

Summary

- The proposition made by UWB is what Bluetooth wireless technology should have been.

- The Bluetooth SIG and WiMedia Alliance have collaborated to support Bluetooth over UWB.
- According to the WiMedia Alliance's website, WiMedia is UWB.
- WiMedia is primarily targeted towards wireless multimedia-specific applications.
- It is abundantly clear that UWB can comfortably accommodate the genre of latency specific applications.
- It should be clear; UWB doesn't need Bluetooth.
- Many have argued that Bluetooth and UWB are competitors.
- Bluetooth has taken several years to become visible to the consumer.
- WiFi is perceived to be ubiquitous.
- WiMedia may achieve similar successes as WiFi, possibly through WUSB.
- USB has been around for almost as long as the PC and the simplicity afforded by such a technology has perpetuated the notion of connectivity as a basic task of plugging one end into another.
- We are already familiar with a technology that has comfortably connected one device to another.
- NFC would have been a more obvious choice as an alliance, as the technology lends itself well as an enabler.
- NFC has alleviated connection set-up and authentication with Bluetooth and WiFi.
- WiMedia intends to populate a host of consumer electronic products and it should avoid the necessity of discovery mechanisms and other such nonsense.
- NFC as a technology enabler would further ensure the simplicity consumers so desperately need.
- It seems that the WiMedia Alliance and the UWB Forum are singing from two different pages.
- The WiMedia Alliance has adopted the MB-OFDM version of UWB.
- The UWB Forum has adopted the DS version.
- We do have to apply a sense of proportion and reality when developing technologies that are targeted to simplify many use cases.
- It is bewildering to read that there are two flavors of UWB.
- UWB can stand on her own two feet and provide an effective and robust wireless technology that will embarrass Bluetooth.
- WiMedia can stand alone and deliver consistent and secure wireless technology branded as WirelessUSB.
- Bluetooth adds another level of complexity, which will ultimately confuse a consumer-base that is already struggling to keep up.
- WiMedia needs to keep a steady hand when launching UWB flavored products, as it really can't afford any potential misunderstanding.

Glossary and Definitions

1G First Generation. First generation telecommunications was only capable of supporting voice traffic. It was susceptible to interference and offered no security; see *2G*, *3G* and *4G*.

2G Second Generation. It is with the growth and deployment of digital capability that has led the way forward to the second generation era. The available frequencies that are open to an analog system are also available to a digital system. The distinction between them is that the digital system uses the frequencies in a different way; see *2G*, *3G* and *4G*.

2.5G Second Generation (Extended). A transitory state of evolution between 2G and 3G technology – GPRS is a 2.5G technology; see *GPRS*.

2.75G Second Generation (Additionally extended).

3G Third Generation. Operators in this era have shifted to a new paradigm who are eager to deliver advanced methods for data-centric applications, such as broadcast quality video – UMTS is a 3G technology; see *1G*, *2G*, *4G* and *UMTS*.

3.5G Third Generation (Extended). A transitory state of evolution between 3G and 4G technology – HSDPA is a 3.5G technology; see *HSDPA*.

3.75G Third Generation (Additionally extended).

3Wire A transport mechanism between a host and a host controller of a Bluetooth-enabled device; see *UART* and *USB*^{2}.

4G Fourth Generation. The fourth generation of cellular technologies will shift to a more data-ready centric environment where users will be able to download a variety of content, such as television for example. It is widely thought of as a conceptual evolution and may, in fact, reveal itself as a convergence of a number of wireless technologies; see *1G*, *2G* and *3G* and *Convergence*.

802.3 A series of IEEE standards that define the PHY and MAC layers for fixed LAN Ethernet; see *Ethernet*, *LAN*, *MAC*^{2}and *PHY*.

802.11 The original standard developed in 1999. The original specification supported 1Mbit/s using the overcrowded 2.4GHz frequency.

802.11a A 5GHz solution offering a data rate of up to 54Mbit/s, which was also offered in 1999.

802.11b The most prolific and widely adopted specification, which comprised a number of amendments to the original specification. It was backward compatible with the original specification, but additionally offered 5.5Mbit/s and 11Mbit/s.

802.11c A lesser known specification, but plays a crucial role within the WiFi genre of products as it enables wireless bridging between access points.

802.11d Again a lesser known specification, but dominates much of the WiFi technology in use today as it provides harmonization within countries that are unable to use WiFi.

802.11e An increasingly predominant specification that ensures your WiFi products sustains a good quality of service.

802.11g Another prolific and widely adopted technology that offered backward compatibility with 802.11b. It emerged in 2003 offering data rates of up to 54Mbit/s.

802.11h A standard that was specifically developed to overcome interference with the 802.11a specification, as there were issues with the 5GHz band interfering with satellite and other radio equipment.

802.11i The specification primarily overcomes issues surrounding WiFi security and emerged circa 2004.

802.11j A specification that was specifically drafted for the Japanese market to accommodate their rules regarding radio.

802.11k With the prevalence of WiFi-enabled access points this specification was developed to enhance access point selection where multiple services are offered and is expected to be available in 2007.

802.11m Intriguingly, this specification is a proposal by the 802.11 working group to ensure that all the specifications within the 802.11 family are maintained and are up-to-date; the IEEE began keeping their house in order back in 1999.

802.11n Individually, this specification will keep other personal-area technologies on its toes, as it is set to compete with wireless technologies that will offer audio/video capability. It will be available in 2007 and uses the 2.4GHz band offering a data throughput of up to an amazing 300MBit/s.

802.11p Another exciting specification that specifically targets the vehicle industry, not just your cars, but trains, airplanes and so on, and is expected to be published circa 2008.

802.11r This specification complement's 802.11k, as it alleviates issues surrounding roaming when presented with multiple services.

802.11s A specification that accommodates mesh networking. The standard is expected to be available in 2008.

802.11t WiFi has populated numerous homes and offices and, as such, this specification ensures future reliability of the technology with its *Wireless Performance Prediction* (WPP) test method.

802.11u WiFi increasingly finds itself integrated into numbers of consumer electronics products and, as such, this specification affords a user the ability to context to a network with some or limited services.

802.11v This standard allows administrators to manage and configure their networks and is very much still in its early stages of development.

802.11w 802.11i already offers increased security and authentication; this particular task group is working on amendments to the specification that shall complement 802.11i and will protect management frames within the WiFi protocol.

802.11y Another specification in its very early stages. 802.11y looks at the new available 3.65-3.7GHz bands and how it might offer broadband wireless services.

802.15.3 An IEEE standard that defines the PHY and MAC layers for high-rate WPAN; see *MAC*, *PHY* and *MAC*^{2}.

802.15.3a An extension to the 802.15.3 standard offering an alternative PHY layer for consideration with WiMedia; see *PHY* and *WiMedia*.

802.15.4 An IEEE standard that defines the PHY and MAC layers for low-rate WPAN. The standard is the basis of ZigBee; see *MAC*, *PHY*, *MAC*^{2} and *ZigBee*.

802.15.4b An extension to the 802.15.4 standard offering improved security and an attempt to resolve ambiguities with the original standard; see *ZigBee*.

802.16 An IEEE standard that defines the global exploitation of BWA for the MAN and is commonly referred to as WiMAX; see *BWA*, *MAN* and WiMAX.

802.16e An extension to 802.16 that accommodates the flexible or mobile nature of a device within a MAN context – referred to as Mobile WiMAX; see *MAX* and *Mobile WiMAX*.

802.1X An IEEE standard based upon EAP that typically provides authentication on an AP; see *AP*.

8PSK 8 Phase Shift Key. A modulation scheme that is used with EDGE, as such data rates of up to 384Kbps can be achieved.

A2DP Advanced Audio Distribution Profile (Bluetooth).

Access Point A wireless-enabled device that is capable of interconnecting multiple devices wirelessly to form a WLAN. An AP may perform authentication and encryption schemes to authorize connections; see *WLAN*.

ACL Asynchronous Connection-Orientated. A data-specific logical connection made between two or more Bluetooth-enabled devices; see *eSCO* and *SCO*.

Ad hoc A specific mode of operation that permits STAs to informally join a network without the provision of an AP. More generically, it refers to the ability of a user to connect to a LAN where typically the LAN consists of a trusted group stations; see *AP*, *LAN* and *STA*.

AIB APS Information Base. In the ZigBee protocol stack this refers to the collection of managed objects within the APS; see *Application Objects* and *APS*.

AID Association Identifier.

Alphabet Soup A phrase that has been used to coin the collection of letters that are associated with the IEEE 802.11 specifications.

AMPS Advanced Mobile Phone Standard. A 1G analog cellular technology; see *1G* and *D-AMPS*.

AP Access Point, see *Access Point*.

APL Application Layer; see *Application Layer*.

Application Framework In ZigBee, the application framework is a conceptual storage facility which houses the application objects of a given node; the application framework has a number of defined interfaces, such as ZDO, and is an integral component of the ZigBee protocol stack; see *Application Objects* and *ZDO*.

Application Layer In ZigBee, an application layer is the formation of the application framework, ZDO and APS, which uniquely defines a specific application; see *APS* and *ZDO*.

Application Objects In ZigBee, the application objects are units contained within the application framework on a node that is defined by the profile developer or manufacturer; see *Application Framework*.

Application Support Sub-layer In ZigBee, the application support sub-layer provides an interface to the NWK and APL layers; see *APL* and *NWK*.

APS Application Support Sub-layer; see *Application Support Sub-layer*.

APSDE Application Support Sub-layer Data Entity (ZigBee).

APSDE-SAP APSDE Service Access Point (ZigBee).

APSME Application Support Sub-layer Management Entity (ZigBee).

APSME-SAP APSME Service Access Point (ZigBee).

AS Authentication Server.

ASB Active Slave Broadcast. An ASB is used when a Bluetooth master wishes to communicate with many active Bluetooth slaves; see *PSB*.

ASIC Application-Specific Integrated Circuit. A customized integrated circuit that has been designed for a particular purpose; for example, an 802.11b and a Bluetooth integrated circuit would be ASICs as they have been designed to perform a specific task.

AVRCP Audio/Video Remote Control Profile (Bluetooth).

AutoID Automatic Identifier. An automatic identification system used within RFID technology that enables the automatic tracking and monitoring of tags, typically used in a location to monitor goods in and out of a warehouse, for example; see *RFID* and *Tags*.

Backhaul The backhaul refers to the delivery of a wireless service from a BSC which is typically connected to a fixed infrastructure, to a base station or an AP; see *AP* and *BSC*.

Basic Rate The basic rate data service offered in Bluetooth wireless technology, typically offering a data rate of up to 1Mbit/s; see *Bluetooth* and *Enhanced Data Rate*.

BD_ADDR Bluetooth Device Address; see *MAC*[1].

BER Bit Error Rate.

BIP Basic Imaging Profile (Bluetooth).

Bluetooth A cable replacement technology that utilizes the overcrowded ISM 2.4GHz radio spectrum. Bluetooth wireless technology has enjoyed moderate success within the cellular phone and headset market; see *ISM*.

BoM Bill of Materials. A BoM is the constitution of a product's parts or components, for example its electronics make-up (silicon, resistors, capacitors) and its casing (plastics).

Bonding A term used within Bluetooth wireless technology. It demonstrates the user's intent to pair with one or more Bluetooth-enabled devices; see *Bluetooth* and *Pairing*.

BPP Basic Printing Profile (Bluetooth).

BPSK Binary Phase Shift Keying; see *8PSK*.

BSC Base Station Controller. A unit that is typically connected to a fixed infrastructure and wireless connected to a base station or an AP; see *Backhaul*.

BSS Basic Service Set. A BSS is pivotal in a WiFi network as it indicates the radio range in which a number of stations can share a connected service; see *STA* and *WiFi*.

BT Bandwidth-bit Time.

BT Bluetooth; see *Bluetooth*.

BSSID Basic Service Set Identifier. A 48-bit MAC address that is used to uniquely identify a BSS and an IBSS on a WLAN network; see *BSS*, *IBSS*, *MAC*[1] and *SSID*.

BWA Broadband Wireless Access; see *WiMAX*.

CBC-MAC Cipher-block Chaining with Message Authentication Code. A cipher scheme used to encrypt plaintext.

CCA Clear Channel Assessment. A mechanism used, prior to a transceiver transmitting a payload, to determine if a channel is clear; see *CSMA-CA* and *CSMA-CD*.

CCK Complementary Code Keying.

CCMP CTR with CBC-MAC Protocol.

CDMA Code Division Multiple Access.

Checksum A value that is appended to a data packet prior to transmission. It ensures that the receiving device has not received corrupted or invalid data.

Chip[1] A chip synonymously referred to as an integrated circuit or semiconductor; essentially, a microprocessor that has a duty to perform a number of tasks; see *ASIC* and *Chip*[2].

Chip[2] A British cuisine – almost similar, but fatter and tastier than the French equivalent (fries), often accompanied with fish and lashings of tomato ketchup. Also known as a potato chip (US) and a tortilla chip (Mexico), and equally as tasty.

CID Channel Identifier. The identification of an L2CAP logical endpoint used within the Bluetooth protocol stack; see *L2CAP*.

CIP Common ISDN Access Profile (Bluetooth).

Coexistence A classic term thrown around in the very early days of wireless emergence. It specifically refers to the ability of multiple wirelessly enabled devices to coexist in proximity without degrading the respective quality of another wireless device; see *Interoperation*.

Convergence The amalgamation of a number of wireless technologies into a singular device that manifests itself as a single application to the consumer; for example, if a consumer wishes to surf the Internet the medium underlying the ability to provide the Internet service will remain transparent to the consumer, but the combination of technologies will afford the consumer a single experience; see *Coexistence*.

CRC Cyclic Redundancy Check; see *Checksum*.

CSD Circuit Switched Data; see *HSCSD*.

CSMA-CA Carrier Sense Multiple Access with Collision Avoidance. A technique used in wireless LANs that is used to ensure that a payload transmits when a channel (wireless) is clear and no other station is transmitting; see *CSMA-CD* and *Station*.

CSMA-CD Carrier Sense Multiple Access with Collision Detect. A technique used in fixed LANs that is used to ensure that a payload transmits when a channel (fixed) is clear and no other station is transmitting; see *CSMA-CA*.

CTP Cordless Telephony Profile (Bluetooth).

D-AMPS Digital Advanced Mobile Phone Standard. The onset of 2G technology; a digital revision of AMPS; see *AMPS*.

DCF Distributed Coordination Function. A default mechanism for a station (or a wireless node) that is used in a WLAN to determine if other stations are transmitting before it transmits itself; see *CS* and *WLAN*.

DDR Dual Data Rate.

Downlink A downlink represents the communication pathway between a server and client device, for example; see *Uplink*.

DHCP Dynamic Host Configuration Protocol. The DHCP protocol affords the allocation of IP address, as well as a host of configuration parameters, such as DNS addresses and subnet masks; see *DNS*, *IP* and *subnet mask*.

Distributed Application In ZigBee a series of nodes will be distributed around an area such as a home or office. For example, a switch on one node will communicate with a light on another node, in turn, they collectively form a simple light switch (on/off) application.

DNS Domain Name System; see *DHCP*.

DoS Denial of Service. A DoS is where a hacker disrupts a system by disabling users to access a service.

DS Distribution System (WiFi).

DSM Distribution System Medium (WiFi).

DSRC Dedicated Short Range Communications. A short range radio communications technology specifically designed for automotive applications; see *ITS*.

DSS Distribution System Service (WiFi).

DSSS Direct Sequence Spread Spectrum. A modulation scheme where the signal is spread over the allocated bandwidth.

DUN Dial-up Networking (Profile).

E_0 A stream cipher algorithm used in Bluetooth that individually encrypts digits within a plaintext payload; see *Bluetooth*.

EAP Extensible Authentication Protocol (WiFi).

EAPOL Extensible Authentication Protocol over LAN (WiFi).

EDGE Enhanced Data GSM Evolution. A technology that supports greater throughput for data-centric applications; see *GPRS*, *GSM* and *HSDPA*.

EDR Enhanced Data Rate, see *Enhanced Data Rate*.

EMCA European Computer Manufacturers Association.

Endpoint An endpoint in a ZigBee protocol stack context refers to a logical connection that is made between nodes that share common applications; see *Application Framework*.

Enhanced Data Rate An extended version of the Basic Rate used for data applications within Bluetooth. An EDR-enabled device is capable of supporting data rates of up to 3Mbit/s; see *Basic Rate* and *Bluetooth*.

Extended Rate PHY A modification (WiFi) that has been made to the PHY layer of the OSI Model; see *OSI Model*, *PHY* and *WiFi*.

eSCO Extended Synchronous Connection-Orientated. eSCO is an audio/voice-centric logical connection medium in Bluetooth supporting a faster and more reliable data throughput; see *ACL*, *Bluetooth* and *SCO*.

ESDP Extended Service Discovery Profile (Bluetooth).

Ethernet A fixed LAN technology based upon the IEEE 802.3 standard; see *NIC*.

ETSI European Telecommunications Standards Institute.

FAX FAX Profile (Bluetooth).

FCS Frame Check Sequence; see *Checksum*.

FDD Frequency Division Duplex.

FDMA Frequency Division Multiple Access.

FFD Full Function Device. An end-device within a ZigBee network topology; see *RFD*.

Feistel A Feistel is a cryptographic block cipher; see *TEA*.

Felcia A Sony smart-contact-less-card based upon NFC technology; see *NFC*.

FM Frequency Modulation.

FOMA Freedom of Mobile Multimedia Access. A brand name given to the NTT DoCoMo 3G technology service in Japan.

FSK Frequency Shift Keying.

FTP File Transfer Profile (Bluetooth).

Frequency Hopping A scheme used in Bluetooth and other wireless technologies that hops between channels if a given channel is already being used. A master and slave device will agree on how to do this.

GAP Generic Access Profile (Bluetooth).

GFSK Gaussian Frequency Shift Keying.

GOEP Generic Object Exchange Profile (Bluetooth).

GMK Group Master Key (WiFi, WPA2).

GMSK Gaussian Minimum Shift Keying.

GPRS General Packet Radio Services. A 2.5G technology that supports greater throughput for data-centric applications; see *EDGE*, *HSDPA*, *GSM* and *UMTS*.

GSM Global System for Mobile Communications. A 2G digital cellular technology that is widely used throughout the world; see *EDGE*, *GPRS*, *HSCSD* and *UMTS*.

GTK Group Transient Key. A GTK is generated as the result of a GMK (WiFi).

HC Host Controller (Bluetooth); see *3Wire*, *SD*, *UART* and *USB*[2].

HCI Host Controller Interface (Bluetooth); see *3Wire*, *SD*, *UART* and *USB*[2].

HCRP Hard Copy Replacement Profile (Bluetooth).

HFP Hands-free Profile (Bluetooth).

HID[1] Human Interface Device. Any device that enables a human to input information to a computer is an HID; for example, a keyboard and mouse are HID devices.

HID[2] Human Interface Device (Profile).

Hotspot A hotspot is a location which is covered by an AP that allows a user to connect to a wireless service, such as the Internet.

HR/DSSS High-rate DSSS; see *DSSS*.

HSCSD High Speed Circuit Switched Data. A modification that has been made to GSM to support greater data throughput over the cellular network; see *EDGE*, *GPRS*, *GSM* and *UMTS*.

HSDPA High-speed Downlink Packet Access. A modification made to WCDMA technology to further increase data throughput for data-centric applications. HSDPA is considered to be a 3.5G technology; see *EDGE*, *GPRS*, *GSM* and *UMTS*.

HSP Headset Profile (Profile).

IBSS Independent Basic Service Set. An IBSS is an ad hoc WiFi-enabled LAN where STAs can informally join a network without the provision of an AP; see *AP*, *BSS*, *LAN*, *STA* and *WiFi*.

IC Integrated Circuit.

ICP Intercom Profile (Bluetooth).

ICV Integrity Check Value; see *Checksum*.

IEEE Institute of Electrical and Electronic Engineers.

IF (low-) low-Intermediate Frequency.

i-Mode A Japanese service which is increasingly becoming popular throughout the world; see *Wireless Application Protocol*.

Infrared A short-range wireless medium that uses Infrared as its transport medium. A successful wireless technology that has been mimicked in its application-base by Bluetooth; see *Bluetooth*.

Interoperation Interoperation is the ability for one device to successfully communicate with another irrespective of manufacturer; see *Coexistence*.

IP Internet Protocol. A commonplace protocol that is used to enable communication between client and server-based packet-switched networks such as the Internet.

IrDA Infrared Data Association; see *Infrared*.

IS-54 Interim Standard 54. A standard that outlines the DAMPS technology; see *IS-95*, *CDMA*, *IS-136* and *D-AMPS*.

IS-95 Interim Standard 95. A standard that outlines the CDMA digital technology; see *IS-54*, *AMPS*, *IS-136* and *D-AMPS*.

IS-136 Interim Standard 136. As IS-54, but with additional features to include text messaging and CSD; see *IS-54*, *AMPS*, *IS-95* and *CDMA*.

ISDN Integrated Services Digital Network.

ISM Industrial, Scientific and Medical.

ISP Internet Service Provider. A company that typically offers Internet access and other services; see *WISP*.

ITS Intelligent Transportation System. A worldwide proposal that will enable a multiple number of transport vehicles and its associated infrastructure to carry information; see *DSRC*.

IV Initialization Vector. A 24-bit integer used in creating a 64-bit secret WEP key value; see *WEP*.

JDC Japanese Digital Cellular, see *PDC*.

KVP Key Value Pair (service type). A basic command/control messaging mechanism used within the ZigBee protocol stack; see *MSG*.

L2CAP Logical Link Control and Adaptation Protocol (Bluetooth).

LAN Local Area Network. A fixed structure of interconnecting computers or devices sharing services; see *WLAN*.

LAP[1] LAN Access Profile (Bluetooth).

LAP[2] Lower Address Part (Bluetooth).

LC Link Controller. A layer one component (OSI-based) of the Bluetooth protocol stack; see *PHY* and *OSI Model*.

LM Link Manager. A layer two component (OSI-based) of the Bluetooth protocol stack, see *MAC*^{2} and *OSI Model*.

LMP Link Manager Protocol (Bluetooth).

LPP Local Positioning Profile (Bluetooth).

LSB Least Significant Bit (or Byte).

LT_ADDR Logical Transport Address (Bluetooth).

MAC^1 Media Access Control (address). A 48-bit address that uniquely identifies a device at a physical location in a network.

MAC^2 Medium Access Control (layer). The MAC forms the data link layer (second layer) of the OSI model and sits above the PHY layer; see *OSI Model* and *PHY*.

MAN Metropolitan Area Network. A MAN is a large-scale hotspot equivalent; see *Hotspot*.

ME Management Entity.

MMS Multimedia Messaging Service.

MIC Message Integrity Code. In a wireless communication system a MIC is often appended to a payload to ensure the integrity of the data being received; see *Checksum*.

Michael See *MIC*.

Mesh Network A mesh is a web or lattice structure that is interconnected. A ZigBee and Z-Wave network may form a mesh structure.

MLME MAC Layer Management Entity (WiFi); see *MAC*^{2}.

Mobile WiMAX See WiMAX.

MPDU MAC Protocol Data Units (WiFi); see *MAC*^{2}.

MSB Most Significant Bit (or Byte).

MSC Message Sequence Chart.

MSDU MAC Service Data Units (WiFi); see *MAC*^{2}.

MSG Message. A more dynamic command/control messaging mechanism used within the ZigBee protocol stack that uses the underlying KVP service, but remains application-specific; see *KVP*.

Multicast Most Significant Bit (or Byte).

NAP Non-significant Address Part (Bluetooth).

NAS Network Access Server.

NAV Network Allocation Vector. A virtual carrier-sense function that affords the MAC sub-layer of a WLAN the ability to predict the traffic on the network before it transmits a new payload; see *DCF*, *MAC*[2] and *WLAN*.

NFC Near Field Communications.

NFMC Near Field Magnetic Communication. A technology that is Aura Communications Technology which provides the ability to support wireless stereo headset functionality; see *NFC*.

NIC Network Interface Card. A fixed unit typically fitted into your PC via the PCI slot of your computer that supports the intercommunication of your LAN; see *WNIC*.

Node A node is a self-organizing, self-sustaining wireless device (ZigBee or Z-Wave) that communicates with other nodes. It is the collection of these nodes that form the intended application; see *Distributed Application*.

NWK Network (ZigBee); see *ZigBee*.

OBEX Object Exchange (Bluetooth). A communications protocol that is used by Bluetooth wireless technology to support a host of Infrared legacy applications; see *Infrared*.

OpCode Operation Code. An OpCode is used to denote the type of PDU being sent in the LM layer of a Bluetooth protocol stack; see *Bluetooth*.

OPP Object Push Profile (Bluetooth).

OSI Open Systems Interconnect.

OSI Model Open Systems Interconnect Model. A paradigm used within communication protocol that enables interoperation. The OSI model is made up of seven layers; see *Interoperation*.

OTG On The Go. A derivative of the USB technology that enables multiple devices to be connected to one another without the support of a computer; see *USB*.

PAE Portal Access Entity.

PAN[1] Personal Area Network. A number of computers or other devices that are connected on an ad hoc basis; see *Ad hoc*.

PAN^2 Personal Area Network Profile (Bluetooth).

Pairing (Bluetooth) A procedure that is undertaken when two or more Bluetooth-enabled devices exchange a Bluetooth passkey – this typically leads on to authentication and encryption; see *PIN*.

Passkey (Bluetooth) A passkey is typically used within the Bluetooth context to authorize a user access to another Bluetooth-enabled device; see *Bluetooth*.

PBCC Packet Binary Convolutional Code.

PC Point Coordinator. A mechanism used in an AP of a WLAN to individually poll each connected station to determine which one can transmit; see *DCF* and *PCF*.

PCF Point Coordination Function. A mechanism used within an AP which is used to determine if other stations are transmitting; see *AP* and *DCF*.

PCI Peripheral Component Interconnect.

PCS Personal Communication Services.

PDA Personal Digital Assistant.

PDC Personal Digital Cellular. A Japanese derivative of D-AMPS and GSM; see *D-AMPS* and *GSM*.

PDU Protocol Data Unit.

Personal-area With the introduction of a new range of wireless-enabled applications that define a greater sense of personal mobility and freedom uniquely captures the personal-area technology era. Technologies such as Bluetooth, WiFi, ZigBee and so on, afford the user greater flexibility in their personal and/or working environment. Personal-area technology enables users to create their own personal communications environment, which may comprise a notebook wirelessly connected to a network and a cell phone that utilizes a Bluetooth-enabled headset; see *Wide-area*.

PHY Physical (layer). The physical layer forms the point at which software (a protocol stack) interacts directly to hardware (a radio, for example); see *OSI Model*.

PIN Personal Identifier Number.

PLCP Physical Layer Convergence Procedure. A sub-layer of the PHY layer within the WiFi protocol stack; see *PHY* and *PMD*.

PLME Physical Layer Management Entity (WiFi).

PMD Physical Medium Dependent. A sub-layer of the PHY layer within the WiFi protocol stack; see *PHY* and *PLCP*.

PMK Pairwise Master Key.

PN Pseudo-Noise.

PPDU PHY Product Data Unit; see *PHY*.

PRNG Pseudo-random Number Generator.

PRoC Programmable Radio on a Chip.

PSB Parked Slave Broadcast. The PSB allows the Bluetooth master to communicate with many Bluetooth parked slaves; see *ASB*.

PSDU PLCP Service Data Units; see *PLCP*.

PSK Phase Shift Keying; see *8PSK*.

PSTN Public Switched Telephone Network.

PTK Pairwise Transient Key.

QPSK Quadrature Phase Shift Key; see *8PSK*.

RF Radio Frequency.

RFCOMM A layer within the Bluetooth protocol stack that emulates a serial port; see *Bluetooth*.

RFD Reduced Function Device. An end-device within a ZigBee network topology; see *FFD*.

RFID Radio Frequency Identification. A wireless technology that is primarily used for tracking and tracing of products and people. It is also used in smart payment systems; see *NFC*.

RS232 A telecommunications standard that enables serial devices to communicate with one another; see *RFCOMM*.

RSNA Robust Security Network Association.

RSSI Received Signal Strength Indicator.

SAR Segmentation and Reassembly. Typically a layer within the OSI model may have the responsibility to perform SAR. It specifically refers to the ability of a layer to proportion a payload into transmittable units that the interfacing layer can handle. The same layer, at the peer device, will also undertake the responsibility of the reassembly; see *OSI Model*.

SCO Synchronous Connection-Orientated. SCO is an audio/voice-centric logical connection medium in Bluetooth; see *ACL* and *eSCO*.

SD Secure Digital. A transport layer used within Bluetooth technology to enable a host and host controller to communicate with each other using flash memory technology; see *UART, USB*^{2} and *SDA*.

SDA Secure Digital Association (www.sdcard.org).

SDAP Service Discovery Application Profile.

SDP Service Discovery Protocol.

SDT SD Transport (Bluetooth); see *HCI*.

SDU Service Data Unit.

SFD Start Frame Delimiter.

SIG Special Interest Group (Bluetooth). A non-profit organization that mandates the future growth and application-base of Bluetooth wireless technology; see *Bluetooth*.

SIM^1 SIM Access Profile (Bluetooth).

SIM^2 Subscriber Identity Module. A smartcard that is fitted into a cellular phone that identifies the user across a cellular network.

SIS SUC Id Server.

SLIP Serial Line Internet Protocol. A protocol that is based upon RFC1055 and is used to frame data payloads over a serial interface. In particular, this protocol is used within the 3Wire UART transport layer within Bluetooth technology; see *UART*.

SMS Short Message Service.

SMSing Short Message Servicing.

SoC System on a Chip.

SOHO Small Office/Home Office.

SPP Serial Port Profile (Bluetooth).

SRA Source Routing Algorithm.

SSID Service Set Identifier. A unique field that is included within the MAC frame and is used to identify a packet. The identifier is made up of thirty-two alphanumeric octets, which is typically identified by a user when connecting to an AP; see *AP*, *BSSID* and *MAC*^{2}.

SSS Security Service Specification (ZigBee). A software entity within the ZigBee protocol stack that manages authentication and encryption for ZigBee-enabled devices.

STA Station. A station is a computer or other device that can connect to a WLAN through an AP; see *AP*, *BSS* and *WLAN*.

Subnet Mask The division of LANs on a single site can be achieved through the assignment of a subnet mask. A mask is assigned to every computer that has an IP address where a section of the IP address is allocated to the sub-network; see *IP* and *LAN*.

SUC Static Update Controller.

Synch Synchronization Profile (Bluetooth).

Tag(s) An RFID or NFC device that contains sufficient information that conveys data pertaining to a product or person; see *RFID* and *NFC*.

TCS Telephony Control System (Bluetooth).

TDD Time Division Duplex.

TDMA Time Division Multiple Access.

TD-SCDMA Time Division-Synchronous Code Division Multiple Access.

TEA Tiny Encryption Algorithm. A simple block cipher that is easy to deploy and implement; see *Feistel*.

Texting Short Message Service.

TID Transaction ID. A bit that is set to 1, to denote that a LMP PDU was initiated by a Bluetooth slave and conversely, if set to 0, denotes that a LMP PDU was initiated by the Bluetooth master; see *LMP* and *PDU*.

TKIP Temporal Key Integrity Protocol.

Transponder See *Tag*.

UAP Upper Address Part (Bluetooth).

UART Universal Asynchronous Receiver Transmitter. A transport layer used within Bluetooth technology to enable a host and host controller to communicate with each other; see *SD* and *USB*.

UHF Ultra-high Frequency.

Ultra-Wideband A definitive technology that would ultimately outshine and disband Bluetooth, but as a result of a dichotomy of UWB solutions, we will ultimately witness a battle that will ensue a time akin to Beta vs. VHS.

UMTS Universal Mobile Telecommunications Service.

Uplink A downlink represents the communication pathway between a client and server device, for example; see *Downlink*.

USB[1] Universal Serial Bus. The USB has been around for almost as long as the PC and the simplicity afforded by such a technology has perpetuated the notion of connectivity as a simple means of plugging one end into another; see *OTG* and *WirelessUSB.*

USB[2] Universal Serial Bus (Bluetooth). A transport layer used within Bluetooth technology to enable a host and host controller to communicate with each other; see *SD* and *UART*.

UWB Ultra-wideband; see *Ultra-Wideband*.

VCO Voltage Controlled Oscillator.

VCP Video Conferencing Profile (Bluetooth).

VDP Video Distribution Profile (Bluetooth).

VoIP Voice over Internet Protocol.

VoWAN Voice over WAN.

VoWiFi Voice over Wireless Fidelity; see *Wireless Fidelity*.

VPN Virtual Private Network.

WAP[1] Wireless Application Protocol.

WAP[2] Wireless Access Point; see *Access Point*.

War-Chalking The processes involved in identifying vulnerable wireless networks are known as War-Walking, War-Driving and War-Storming (or Flying). Hackers use a series of symbols derived from hoboism to identify such networks (War-Chalking*).*

War-Driving See *War-Chalking*.

War-Storming (or Flying) See *War-Chalking*.

War-Walking See *War-Chalking*.

WarXing The collective term that encompasses the utilized mode of transportation of hacking into a wireless network; see *War-Chalking*.

WAVE Wireless Access in Vehicular Environments.

WCDMA Wideband Code Division Multiple Access.

WEP Wired Equivalent Privacy. WEP is an initial encryption scheme offered with WiFi which utilized the RC4 algorithm, but failed as a number of hackers revealed its shortcomings; see *WPA*.

Wide-area (wireless communication) More established or wide-area technologies, such as, cellular and satellite are tried and trusted communication technologies that have been around for many years. We've come to know wide-area communications as *telecommunications*, since wide-area is synonymous with connectivity over greater distances; see *Personal-area*.

WiFi Wireless Fidelity; see *Wireless Fidelity*.

WiFi Alliance The non-profit organization, which mandates the future scope of WiFi. It additionally undertakes the effort required to ensure that all WiFi-enabled products comply with their certification programme; see *Wireless Fidelity*.

WiMAX Wireless Metropolitan Area Network. A BWA medium enabling consumers utilizing a MAN service to access the Internet, for example whilst on the move; see *MAN*.

WiMedia According to the WiMedia Alliance, WiMedia is Ultra-wideband. A technology that is targeted for wireless multimedia applications; see UWB.

Wireless Application Protocol An open standard that permits connectivity for a mobile device, such as a cellular phone or PDA, to access the Internet or other web-based service; see *i-Mode*.

Wireless Fidelity Wireless Fidelity is nowadays a brand name, trademarked and licensed by the WiFi Alliance, which undertakes the certification of the numerous 802.11 genre of products. In essence, it has manifested itself as the de facto wireless technology for the everyday user; see *WiFi Alliance*.

Wireless An era of voice and data communication technologies that utilizes radio waves as a transport medium, in turn, enabling electronic devices to exchange a variety of information without cables, transparently and effortlessly; see *Personal-area* and *Wide-area*.

WirelessUSB WUSB is the next generation of consumer-centric wireless technology. WiMedia and Cypress Semiconductors have both mandated such technology that will revolutionize USB technology; see *USB*, *UWB* and *WiMedia*.

Wireless Sniffer A wireless device that may be capable of intercepting the intercommunication of wireless devices. A sniffer is expected to read and understand the information being exchanged enabling a hacker to glean personal information.

WISP Wireless Internet Service Provider. A company that typically offers Internet access and other services through a hotspot (AP); see *AP*, *Hotspot* and *ISP*.

WLAN Wireless LAN. A LAN that has one or more APs connected to it, in turn, providing the same features of a fixed LAN, but wirelessly; see *LAN*.

WMM WiFi Multimedia (Power Save). A revision to the 802.11 series of specifications, which encourages data to be transmitted in the shortest time possible, in turn, enabling a device to go to sleep much more quickly.

WNIC Wireless Network Interface Card. A wireless client device that is fitted to a computer and mimics the behavior of a NIC; see *NIC*.

WPA WiFi Protected Access is an early adopted specification to help overcome initial fears surrounding WLAN; see *WEP*.

WPA2 WiFi Protected Access 2 is the ratified version of the IEEE 802.11i specification; see *WEP*.

WPP Wireless Performance Predication (WiFi).

WUSB WirelessUSB; see *WirelessUSB*.

ZDO ZigBee Device Object. The ZDO within a ZigBee protocol stack has the responsibility for defining specific responsibilities of nodes, in terms of their behavior, in addition to performing service and device discovery procedures to learn of other similarly-enabled devices in proximity.

ZigBee A low-cost and low-power embryonic wireless technology that aims to penetrate the smart home environment, security and home control are some examples. The ZigBee Alliance are in the process of drafting improvements to the current revision of the specification.

Z-Wave A competitive home control technology to ZigBee provided by ZenSys that have already penetrated the smart home context and seems to be further advanced than other would-be technologies.

Bibliography

Barken, L., *How Secure is Your Wireless Network? Safeguarding Your WiFi LAN*, First Edition, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2003.

Bluetooth Special Interest Group, "Specification of the Bluetooth System," Volumes 1, 2 and 3, Version 2.0, November 2004.

Bluetooth Special Interest Group, "RFCOMM with TS 07.10: Serial Port Emulation," Part F:1, Version 1.1, June 2003.

Bluetooth Special Interest Group, "IrDA Interoperability," Part F:2, Version 1.1, February 2001.

Bluetooth Special Interest Group, "Telephony Control Protocol Specification: TCS Binary," Part F:3, Version 1.1, February 2001.

Cable Guy (The), "WiFi Protected Access (WPA) Overview," Microsoft TechNet, March 2003.

Cable Guy (The), "WiFi Protected Access Data Encryption and Integrity," Microsoft TechNet, November 2004.

Cambridge Broadband Limited, "Understanding Range and Coverage for WiMAX Systems," A Cambridge Broadband White Paper, Version 0.5, June 2005.

Carruthers, S., "G! What happened to next-generation wireless networking?" HUBCanada.com, November 2003.

Clint, S. and Collins, D., *3G Wireless Networks*, First Edition, McGraw-Hill Telecommunications, Two Penn Plaza, NY, USA, 2002.

Dornan, A., *The Essential Guide to Wireless Communications Applications: From Cellular Systems to WAP and M-Commerce*, First Edition, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

ECMA International, "Near Field Communications White Paper," 2004.

Edney, J. and Arbaugh, W. A., *Real 802.11 Security: WiFi Protected Access and 802.11i*, First Edition, Addison-Wesley, Boston, MA, USA, 2003.

Gast, M. S., *802.11 Wireless Networks: The Definitive Guide*, First Edition, O'Reilly & Associates, Sebastopol, CA, USA, 2002.

Geier, J., "802.11 MAC Layer Defined," wi-fiplanet.com, June 2002.

Gratton, D. A., *Bluetooth Profiles: The Definitive Guide*, First Edition, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2002.

Gratton, S. J. and Gratton, D. A., *Marketing Wireless Products*, First Edition, Butterworth-Heinemann (an imprint of Elsevier), Oxford, UK, 2004.

Harte, L., Levine, R. and Kikta, R., *3G Wireless: Demystified*, First Edition, McGraw-Hill Telecommunications, Two Penn Plaza, NY, USA, 2002.

IEEE Computer Society, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications," IEEE Std. 802.11-1999, IEEE, 3 Park Avenue, NY, USA, Reaffirmed June 2003.

IEEE Computer Society, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Higher-speed Physical Layer Extension in the 2.5GHz band," IEEE Std. 802.11b-1999, IEEE, 3 Park Avenue, NY, USA, January 2000.

IEEE Computer Society, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 4: Further Higher Data Rate Extension in the 2.5GHz Band," IEEE Std. 802.11g-2003, IEEE, 3 Park Avenue, NY, USA, June 2003.

IEEE Computer Society, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: High-speed Physical Layer in the 5GHz band," IEEE Std. 802.11a-1999, IEEE, 3 Park Avenue, NY, USA, 1999.

IEEE Computer Society, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Amendment 6: Medium Access Control Security Enhancements," IEEE Std. 802.11i-2004, IEEE, 3 Park Avenue, NY, USA, July 2004.

Muller, N. J., *Desktop Encyclopedia of Telecommunications*, Second Edition, McGraw-Hill Telecommunications, Two Penn Plaza, NY, USA, 2000.

Organization for Economic Co-operation and Development, "Working Party on Telecommunications and Information Service Policies: The Implications of

WiMAX for Competition and Regulation," Directorate for Science, Technology and Industry, March 2006.

Rapport, T. S., *Wireless Communications: Principles and Practice*, Second Edition, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2002.

Schiller, J., *Mobile Communications*, Second Edition, Addison-Wesley, Pearson Education Limited, Edinburgh Gate, Harlow, UK, 2003.

Tanenbaum, A. S., *Computer Networks*, Fourth Edition, Prentice Hall PTR, Upper Saddle River, NJ, USA, 2002.

Wexler, J., "How 802.11n backward compatibility works: Integrating 802.11n into your WiFi Network," NetworkWorld.com, February 2006.

WiFi Allaince, "WiFi Protected Access: Strong, standards-based, interoperable security for today's WiFi Networks," 2003.

WiFi Allaince, "WMM Power Save for Mobile and Portable WiFi Certified Devices," December 2005.

WiMedia Alliance, "UWB Standards: WiMedia Alliance White Paper," wimedia.org, June 2006.

ZigBee Alliance, "ZigBee Specification," Version 1.0, December 2004.

ZigBee Alliance, "ZigBee Stack Profiles," Version 1.0, June 2005.

ZigBee Alliance, "ZigBee Device Objects," Version 1.0, December 2004.

ZigBee Alliance, "ZigBee Device Profile," Revision 7, Version 1.0, December 2004.

ZigBee Alliance, "ZigBee Application Framework Specification," Revision 6, Version 1.0, December 2004.

Internet-based references

Mobile/Cellular Technology: *The Website for Mobile Communications* http://www.mobilecomms-technology.com

Wikipedia: *The Free Content Encyclopedia* http://www.wikipedia.com

Privateline.com: *A Tom Farley Production* http://www.privateline.com/

Index

Figures and tables in italics

This page intentionally left blank